Calhoun: The NPS Institutional Archive

DSpace Repository

Theses and Dissertations | 1. Thesis and Dissertation Collection, all items

2007-06

Multistage security mechanism for hybrid, large scale wireless sensor networks

Katsis, Grigorios

Monterey, California. Naval Postgraduate School

http://hdl.handle.net/10945/3424

Downloaded from NPS Archive: Calhoun

http://www.nps.edu/library

Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

MULTISTAGE SECURITY MECHANISM FOR HYBRID, LARGE-SCALE WIRELESS SENSOR NETWORKS

by

Grigorios Katsis

June 2007

Thesis Advisor:	Murali Tummala
Thesis Co-Advisor:	Gamani Karunasiri
Second Readers:	J. Bret Michael
	Owens Walker

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2007	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Multistage Security Mechanism For Hybrid, Large-Scale Wireless Sensor Networks		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Grigorios Katsis			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Department of Electrical and Computer Engineering Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) Missile Defense Agency		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

A wide area network consisting of ballistic missile defense satellites and terrestrial nodes can be viewed as a hybrid, large-scale mobile wireless sensor network. Building on research in the areas of the wireless sensor networks (WSN) and the mobile ad hoc networks (MANET), this thesis proposes an efficient multistage security mechanism for node and data authentication and data confidentiality. Node authentication is provided by digital signatures and the public key infrastructure (PKI). The TESLA algorithm and IPSec are utilized for data authentication and confidentiality, respectively. Performance analysis and simulation results demonstrate that the proposed mechanism meets the real-time data dissemination requirements of a ballistic missile defense system while maintaining throughput commensurate with unencrypted Internet Protocol (IP).

14. SUBJECT TERMS Wireless Sensor Network, Ballistic Missile Defense, Authentication, Security Mechanism, Digital Signatures, TESLA Algorithm			**15. NUMBER OF PAGES** 80 **16. PRICE CODE**
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

MULTISTAGE SECURITY MECHANISM FOR HYBRID, LARGE SCALE WIRELESS SENSOR NETWORKS

Grigorios Katsis
Lieutenant, Hellenic Navy
B.S., Hellenic Naval Academy, 1997

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN APPLIED PHYSICS

and

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
June 2007

Author: Grigorios Katsis

Approved by: Murali Tummala
Thesis Advisor

Gamani Karunasiri
Thesis Co-Advisor

J. Bret. Michael
Second Reader

CDR Owens Walker
Second Reader

James H. Luscombe
Chairman, Department of Physics

Jeffrey B. Knorr
Chairman, Department of Electrical and Computer Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

A wide area network consisting of ballistic missile defense satellites and terrestrial nodes can be viewed as a hybrid, large-scale mobile wireless sensor network. Building on research in the areas of the wireless sensor networks (WSN) and the mobile ad hoc networks (MANET), this thesis proposes an efficient multistage security mechanism for node and data authentication and data confidentiality. Node authentication is provided by digital signatures and the public key infrastructure (PKI). The TESLA algorithm and IPSec are utilized for data authentication and confidentiality, respectively. Performance analysis and simulation results demonstrate that the proposed mechanism meets the real-time data dissemination requirements of a ballistic missile defense system while maintaining throughput commensurate with unencrypted Internet Protocol (IP).

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION 1
A. THESIS OBJECTIVE 2
B. RELATED WORK 3
C. THESIS ORGANIZATION 4

II. HYBRID, LARGE-SCALE, WIRELESS SENSOR NETWORK FOR MISSILE DEFENSE 5
A. THE NETWORK 5
1. Network Architecture and Topology 5
2. Network Design Requirements and Constraints 7
a. Real-Time Data Dissemination Requirements 7
b. Satellite Link Characteristics 8
B. SENSORS 11
1. IR Sensors 12
a. IR Photo Detection 13
b. Quantum Well Infrared Photo Detectors (QWIP) 14
2. RF Sensors 16
C. SECURITY 17
1. Symmetric ciphers 19
a. Block Ciphers and Modes of Operation 20
b. Stream Ciphers 21
2. Public Key Cryptography and RSA 22
a. Principles of Public Key Cryptosystems 22
b. The RSA Algorithm 23
3. Message Authentication and Hash Functions 24
a. Conventional Encryption 24
b. Hash Functions 25
c. Message Authentication Codes and HMAC 26
4. Digital Signatures 27
5. IPSec 28
a. IPSec Architecture 28
b. Authentication Header (AH) 29
c. Encapsulating Security Payload (ESP) 29
d. Modes of Operation 30
e. Security Associations (SA) 32
f. Key Management 32
D. SUMMARY 33

III. PROPOSED MULTISTAGE AUTHENTICATION AND CONFIDENTIALITY SCHEME 35
A. DATA CONFIDENTIALITY 36
B. NODE AUTHENTICATION 36
1. Centralized Authentication 36

2. Distributed Authentication 39
C. DATA AUTHENTICATION 40
D. SUMMARY 43
IV. PERFORMANCE ANALYSIS AND SIMULATION 45
A. NODE AND DATA AUTHENTICATION 45
1. Node Authentication Delay 45
2. Data Authentication 46
3. Simulation Results 46
B. DATA CONFIDENTIALITY 51
1. OPNET Implementation 51
2. Simulation Results 52
C. SUMMARY 54
V. CONCLUSIONS 55
A. CONTRIBUTIONS OF THIS THESIS 55
B. RECOMMENDATIONS FOR FUTURE WORK 56
LIST OF REFERENCES 57
INITIAL DISTRIBUTION LIST 61

LIST OF FIGURES

Figure 1. Hybrid, Large-Scale Wireless Sensor Network for ballistic missile defense (From Ref. [9]) 7
Figure 2. Sensor architecture schematic. Ground/Sea-Based and airborne RF sensors in combination with Satellite-Based IR sensors (From Ref. [29]) 11
Figure 3. Blackbody radiation intensity for different temperatures (From Ref. [14]) 13
Figure 4. Band diagram of an intrinsic photo detector (From Ref. [7]) 15
Figure 5. Quantum Well structure (From Ref. [7]) 16
Figure 6. Cipher Block Chaining (CBC) Mode (From Ref. [23]) 20
Figure 7. Stream Cipher Operation (From Ref. [23]) 21
Figure 8. Message authentication using MAC (From Ref. [23]) 26
Figure 9. Authentication Header appended to an IP packet (AH) 29
Figure 10. Encapsulating security payload (ESP) format (From Ref. [23]) 30
Figure 11. AH transport and tunnel mode 31
Figure 12. ESP transport and tunnel mode 32
Figure 13. Centralized node authentication 37
Figure 14. Pseudocode of centralized authentication phase request 38
Figure 15. Pseudocode of centralized authentication phase response 38
Figure 16. Distributed node authentication 39
Figure 17. TESLA Authentication algorithm example 42
Figure 18. JAVA code execution demo 48
Figure 19. Node authentication delays (t_{req} and t_{res}) for (a) encryption and (b) decryption 49
Figure 20. Total node authentication delay (t_{total}) 50
Figure 21. OPNET network topology 51
Figure 22. Average delay versus PRF 53
Figure 23. Throughput versus PRF 54

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. IBMDS platforms and sensors inventory (After Ref. [13]) 6
Table 2. Nominal propagation times for missile defense network links 9
Table 3. Typical radar parameters (After Ref. [29]) 17
Table 4. Comparison of SHA parameters (After Ref. [23]) 25
Table 5. Summary of the IPSec services (After Ref. [21]) 28
Table 6. Notation used to describe the operation of the proposed multi-stage solution (From Ref. [9]) 35
Table 7. OPNET simulation parameters 52

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like first to express my sincere appreciation to Professor Murali Tummala, my thesis advisor, for his patience and guidance through the completion of this thesis. His advice kept me focused and on course, and taught me how to perform research and writing at the postgraduate level.

I would also like to thank my co-advisor and second readers, Associate Professor Gamani Karunasiri, who provided guidance and materials for the sensors section; Professor J. Bret Michael, who provided guidance and advices for subjects related to Missile Defense; and CDR Owens Walker, who helped me to focus my research and writing.

Lastly, and most importantly, I wish to thank Danai, the inspiration of my life. This thesis is dedicated to you.

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The Missile Defense Agency (MDA) is responsible for developing a ballistic missile defense system (BMDS) capable of protecting the U.S. homeland and its allies against inter-continental ballistic missiles (ICBM) launched from anywhere in the world. To accomplish this objective, the BMDS mission requirements include surveillance, target detection, target tracking and discrimination, and kill assessment. These functions are performed by satellites at various orbits, mobile and fixed terrestrial platforms carrying IR and RF sensors, and ballistic missile interceptors for all stages of flight of the ICBM.

All these sensors and platforms must be efficiently networked together, and target information should be transmitted back to a command and control center for decision making and weapon assignment purposes. This implies the need for real-time data exchange despite challenges presented by the hybrid, large-scale network.

There are a number of security-related issues that should be addressed and solved prior to an early implementation of the system. These include node and data authentication as well as data confidentiality. Revealing any portion of the sensitive transmitted information to an untrusted party could degrade the accuracy and the reliability of the BMDS because target data could be deliberately altered or false data information could be inserted into the network.

This thesis proposes a multistage security mechanism that provides node and data authentication as well as data confidentiality to protect the exchanging data from unauthorized viewing by applying encryption in the network layer. A two-stage node authentication is proposed based on digital signatures and public key infrastructure (PKI) because it uses certificate authorities for verification of the new node's authentication credentials. Data authentication is accomplished through the timed efficient stream loss-tolerant authentication (TESLA) protocol, which is in the process of becoming an IEEE standard. Finally, data confidentiality is provided by the IPSec set of protocols.

The performance of the proposed security mechanism is demonstrated using a Java crypto library and an OPNET simulation. A library of cryptographic functions, written in Java, measure the delays associated with the cryptographic algorithms that the proposed mechanism utilizes. Additionally, an OPNET simulation of the network is performed to evaluate the network's throughput and delay performance when IPSec is applied. Performance analysis and simulation demonstrate that the proposed security scheme performs well when compared with unencrypted IP. Delay and throughput evaluation emphasize the expected trade-off between security and overhead and also verify that the real-time data dissemination objective is met.

I. INTRODUCTION

The threat of a nuclear attack has been a challenge to the United States for over fifty years. As technology and access to it continue to evolve, weapons of mass destruction become efficient and more deadly while falling into the hands of an increasingly layer set of potential adversaries. Under the auspices of the Missile Defense Agency (MDA), a system capable of providing protection against intercontinental ballistic missiles (ICBMs) carrying multiple nuclear warheads has been under development for several years [27]. Such a system, identified as the ballistic missile defense system (BMDS) should be able to detect, track, and intercept ballistic missiles launched against the United States and its allies from any location in the world.

An ICBM is a long-range ballistic missile designed for the delivery of nuclear weapon warheads. Its effective range exceeds 5,500 km or more, which allows it to be launched over oceanic distances. Platforms from which an ICBM could be launched vary from protected military silos to submarines and specially constructed mobile trucks. An ICBM follows three phases of flight: boost, midcourse, and terminal. The boost phase lasts from 3 to 5 minutes, and the missile reaches a speed of 7 km/sec. During this phase, the missile is constantly accelerating. When the ICBM reaches an altitude of approximately 1,200 km, the 25-30 minute midcourse phase begins. During midcourse, the missile is capable of deploying anti-detection decoys and countermeasures. As the ICBM reaches its target at an altitude of 100 km, the terminal phase of its trajectory begins [27].

One functional requirement of the BMDS is the capability to intercept an ICBM in all phases of flight. Although midcourse offers several advantages including ample time for detection, weapon assignment and interception, the ability of the ICBM to deploy its countermeasures as well as the possibility of collateral damage or nuclear detonation over friendly territory make this phase challenging. Terminal phase tends to be viewed as a “last choice,” so much work is now focused on the boost phase. The relatively small duration of the boost phase necessitates early detection; therefore, sensors

and interceptors must be deployed in the vicinity of the launching area. Furthermore, the reaction time is minimal and target data have to be transmitted back to the decision maker almost instantly. The significant advantage is that detection during this phase can be accomplished by IR sensors because the ICBM's thermal signature is high due to the plumes produced by its acceleration.

A number of security challenges face any underlying network designed to support a boost phase solution. The target information must be transmitted from the sensors to a command and control center for threat assessment and potential weapon assignment. A complete security solution must provide confidentiality, integrity and authentication for both the data and the communicating entities.

These problems are further complicated by the wireless nature of the transmission medium. In addition to simple eavesdropping, the lack of physical boundaries allows an adversary to intercept and inject rogue data with relatively little effort. An authentication mechanism to validate the credentials revealed by the incoming network nodes as well as an intrusion detection mechanism to identify and restrict access to rogue nodes must be applied. The requirement to deploy sensors near the launching platform further increases the probability of a compromised node attempting to participate in the network.

A. THESIS OBJECTIVE

The objective of this thesis is to propose a multistage security scheme for hybrid large-scale wireless sensor networks for missile defense. The wireless nature of this large-scale network makes security challenging. The lack of physical boundaries complicates the requirements to confirm the authenticity of the communicating nodes, ensure that data from a valid source were not altered during transit and to protect the data from unauthorized viewing. The proposed multistage scheme consists of three separate security mechanisms designed to provide node authentication, data authentication, and data confidentiality. Analysis and simulation are included to demonstrate the delay and throughput performance of the proposed scheme.

B. RELATED WORK

The proposed security mechanism builds on research conducted for traditional wireless sensor networks (WSN) and mobile ad hoc networks (MANET) and applies it to a hybrid, large-scale network for missile defense. Unlike WSN and MANET applications, though, the nodes of this network are interconnected across large propagation distances and are not constrained by limited computational power, lack of memory, or energy limitations.

A number of distributed public key management schemes to achieve node authentication for mobile ad-hoc networks have been proposed. Zhou et al. [34] propose a public key infrastructure (PKI) system in which the certificate authority (CA) private key is shared among nodes that have to cooperate in order to reveal the key. MOCA, proposed in [31] and [32], is an extension to [34] in which the CA is distributed not to the entire set of the nodes but only to those that exhibit physical security and adequacy in computational resources. J. Kong et al. [11] distributes portions of the CA's key among different nodes. Our proposed scheme for digital signatures is based on a PKI infrastructure using strong encryption keys (1024 or 2048 bits in length) of the Rivest-Shamir-Adelman (RSA) algorithm [20], which produces asymmetric keys used for encryption and decryption.

Unlike those designed for node authentication, data authentication protocols used for real-time data exchange must have small authentication delays. BiBa [16] and HORS [19] are one-time signature authentication schemes using one-way functions. Chang et al. [22] solve the problem of storing many hash function operations in these schemes. The TESLA protocol [17], [15] provides efficient broadcast authentication by using one-way key chains and time slots as asymmetric primitives and is in the process of being standardized in the IETF Multicast Security (MSEC) working group [12]. It minimizes the authentication overhead, exhibits robustness in the face of packet losses, and can support links with different propagation delays. The μTESLA protocol [18] is the "micro" version of TESLA, designed specifically for wireless sensor networks.

C. THESIS ORGANIZATION

This thesis is organized as follows. Chapter II describes the hybrid, large-scale network designed to support the ballistic missile defense system. The network real-time data dissemination requirements and link characteristics as well as the desired properties of the IR and the RF sensors are discussed. Security issues are addressed and the necessity of providing a multistage security mechanism for node and data authentication and data confidentiality is explained. A brief description of basic security primitives and protocols is given. Chapter III introduces the proposed multistage security mechanism, and Chapter IV examines the delay and throughput performance of the proposed algorithm through analysis and simulation. Chapter V provides conclusions of this thesis as well as recommendations for future work.

II. HYBRID, LARGE-SCALE, WIRELESS SENSOR NETWORK FOR MISSILE DEFENSE

This chapter examines the network architecture, sensor characteristics, and security considerations. The observations in this chapter will be used to design the proposed security solution of the large-scale wireless sensor networks for missile defense.

A. THE NETWORK

The Missile Defense Agency (MDA) has provided guidelines on network structure and functionalities for the Integrated Ballistic Missile Defense system (IBMDS) [13]. Building on these requirements, we envision a network architecture that relies on reliable, efficient, real-time cooperation between the nodes to provide a layered defense against a wide range of ballistic threats. This section addresses the topology, coverage, link characteristics, and security considerations of such a network.

1. Network Architecture and Topology

A ballistic missile defense system's mission is to detect, track, and destroy one or multiple ballistic missiles launched from any platform and location in the world. A wireless wide-area network comprised of ballistic missile defense sensor platforms providing global coverage must be designed to support this challenging mission. Mission-related functions for this type of network include early warning/detection, real-time target tracking, and secure target data transfer to a command and control center for decision making and weapon assignment.

The proposed hybrid, large-scale network consists of satellite and terrestrial nodes in a 3-tier hierarchical structure positioned to provide global coverage. At the higher tiers, Geostationary Earth Orbit (GEO) and Low Earth Orbit (LEO) satellites with search and track IR sensors are deployed, providing wider fields-of-view and redundancy in the network. Lower tier terrestrial platforms are mobile or fixed RF and IR sensors, such as land-based stations, warships, forward deployment radars (FDR), aircraft, and unmanned air vehicles (UAV).

Ballistic missiles follow a trajectory that consists of three phases: boost, midcourse, and terminal. Although the system should provide protection in all phases of flight, the focus of this work is based on missile engagement during its boost phase. In this phase, the missile countermeasures would not yet be deployed, the low altitude provides a wider selection of weapons, and the likelihood of friendly, collateral damage would be minimized. Accordingly, nodes of our network capable of detecting launches, tracking missile trajectories, and intercepting ballistic targets will be deployed and distributed as close as possible to the enemy's boundaries. Table 1 presents the evolving IBMDS sensors and weapons inventory.

	2005	**2006**	**2007**
WEAPONS			
Ground-Based Interceptors (Long-Range Threat, Midcourse Defense)	10	14	24
Patriot Advanced Capability-3 (Short & Medium Range Threat, Terminal Defense)	325	413	549
Standard Missile-3 Sea-Based Interceptors (Short-to-Intermediate-Range Threat, Midcourse Defense	9	14	21
Aegis Ballistic Missile Defense	2 Cruisers	3 Destroyers 2 Cruisers	7 Destroyers 3 Cruisers
SENSORS (except Existing Defense Support Program Satellites)			
Upgraded Existing Early Warning Radars	2	3	3
Aegis Ballistic Missile Defense Ships (Long Range Surveillance and Track Only)	10 Destroyers	10 Destroyers	7 Destroyers
Sea-Based X-Band Radar		1	1
AN/TPY-2		1	2

Table 1. IBMDS platforms and sensors inventory (After Ref. [13])

An example of a hybrid, large-scale wireless sensor network for missile defense has been proposed by [8] and is shown in Figure 1. Here, the network is comprised of GEOs, LEOs, and terrestrial stations. When a potential target of interest (TOI) is detected, sensor nodes form an Area of Interest (AOI) based on predefined criteria, such as range to the TOI and whether the TOI is inbound or outbound. The AOI is a clustering mechanism designed to facilitate data aggregation and data-centric routing within the

network. As the target moves through the sensors field, nodes make local (distributed) decisions to join or exit the AOI, and the AOI can be considered to "virtually" move in time.

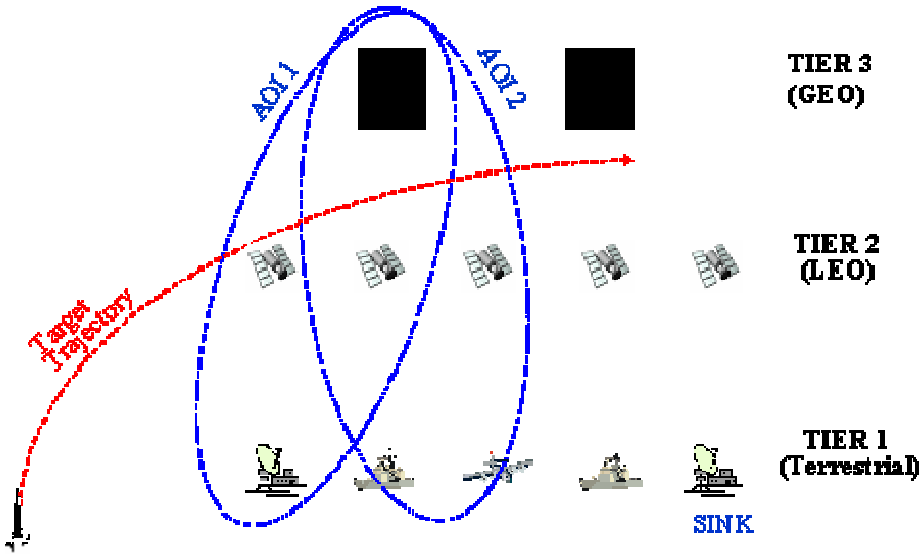


Figure 1. Hybrid, Large-Scale Wireless Sensor Network for ballistic missile defense (From Ref. [9])

2. Network Design Requirements and Constraints

In the following sections, the real-time data dissemination requirements generated by the missile defense application and the constraints of the satellite links are examined. The type of data, the manner in which the data are disseminated, and the underlying link characteristics play an important role in optimizing an appropriate security mechanism. For example, data broadcast requires a security mechanism that scales well for large numbers of recipients. Additionally, such a mechanism should be robust in the face of packet losses if applied to a link with high bit error rates (BER).

a. Real-Time Data Dissemination Requirements

Target tracking with the intent of missile engagement in the boost phase imposes stringent real-time delay requirements on the underlying communications

network. By real-time, we mean that there exist defined maximum bounds on the end-to-end latency of the data transmissions. This requirement can be best illustrated by examining the flow of events that must occur during the 3-4 minute boost phase. Upon target detection, target data are broadcast to all the nodes in the network. Nodes inside the AOI pick up the tracking function and route target data through an aggregator back to the command and control center. The command and control center processes the data and assigns an order to the weapon platform to be used for the target engagement. These data continue until the missile is intercepted. Considering the large propagation times associated with the satellite network links, it is critical to avoid processing, routing or security mechanisms that substantially increase the total delay.

b. Satellite Link Characteristics

The topology proposed for the hybrid, large-scale network is comprised of both terrestrial and satellite links. Terrestrial links have been well-studied in the wireless network literature (e.g., IEEE 802.16 standard). Accordingly, this section focuses on the satellite links and their delay, throughput and BER characteristics.

Many communications satellites are located in the Geostationary Orbit (GEO) at an altitude of 35,863 km. Although, three satellites are necessary to achieve global coverage, four are typically used to provide sufficient overlaps. At this altitude, the orbit period is the same as the Earth's rotation period, and the satellite remains fixed over a point on the Earth's surface. Therefore, each ground station is always able to "see" the orbiting satellite at the same position in the sky. The propagation time for a radio signal to travel to a GEO satellite directly overhead is given by

$$t = \frac{s}{c} = \frac{35863\,\text{km}}{3\times10^{8}\,\text{m/s}} = 0.1195\,\text{sec} \qquad (2.1)$$

where s is the satellite altitude and c the speed of light. In communication applications where satellites act as relays for terrestrial nodes, delays are characterized by round trip

propagation times and increase by a factor of two. Furthermore, the satellite propagation delay will be even longer if the link includes multiple hops or if inter-satellite links are used.

The lower orbits associated with LEO satellites require the use of more satellites for constant global coverage. To achieve global coverage, a constellation of at least 16 LEO satellites is required. Typically, twenty satellites are used to provide a sufficient overlap. LEO satellites are usually located at in an altitude band of 500–1500 km. The propagation delay to a LEO orbit ranges from several milliseconds when communicating with a satellite directly overhead to as much as 80 ms when the satellite is on the horizon. Table 2 summarizes the propagation delays for the different satellite links comprising the ballistic missile network.

Link Characteristic	Propagation Distance (km)	Propagation time (sec)
GEO-GEO	66,352	0.22
GEO-LEO	34,863	0.116
LEO-LEO	2,318	0.008
Terrestrial-GEO	35,863	0.12
Terrestrial-LEO	1,000	0.003

Table 2. Nominal propagation times for missile defense network links

A network that consists of both satellite and terrestrial nodes implies the need for both terrestrial-to-satellite and satellite-to-satellite links. Particular emphasis and attention should be given to the satellite-to-satellite propagation times because the missile defense network utilizes interconnected satellite nodes that do not simply act as communication relays between space and earth stations but are an internal part of a larger network.

Satellite communication channels are dominated by two fundamental characteristics: large noise levels and limited bandwidth. The strength of a radio signal falls off as a square of the distance traveled. For a satellite link, the large distance results

in a low signal-to-noise ratio. Additionally, some frequencies are particularly sensitive to atmospheric effects, such as rain attenuation. Satellite channels are especially susceptible to multi-path distortion. Typical bit error rates (BER) for a satellite link today are on the order of 10^{-7} or less [1].

Satellite systems are typically bandwidth-limited, which makes it difficult to trade bandwidth to solve other design problems. In most applications, an asymmetric approach is used, and the downlink channel is provided a greater capacity than the uplink channel. This is because the downlinks are normally intended for broadcasting when the satellites are used as communication relays.

In the context of the wireless network, these satellite link characteristics tend to degrade the performance of acknowledgement-based transport protocols, such as the transmission control protocol (TCP). Due to the large propagation delay of the satellite links, it will take a long time for a TCP sender to determine whether or not a packet has been successfully received at the final destination. Furthermore, TCP has no mechanism to determine whether a packet loss is due to congestion or bit errors. It is primarily designed for links with small BERs, so it assumes packet losses are due to congestion in the network and dramatically reduces the offered load. Thus, the congestion and flow control algorithms incorporated in TCP prevent it from fully utilizing the satellite link, resulting in relatively poor performance [33].

Performing Enhancing Proxies (PEP) is one of the solutions designed to overcome the TCP performance degradation across satellite links [26]. PEP are deployed between the two communicating entities and use techniques, such as acknowledgement handling, speeding up the TCP slow start mechanism, and increasing the congestion window. PEP improves the congestion of the low speed uplink by delaying the transmission of acknowledgments of TCP segments that arrive in bursts or reconstructing acknowledgments if they are lost. PEP can also be used for retransmission of TCP segments when duplicate acknowledgements are received. This function requires additional buffering capabilities. Another useful function is tunneling in which messages are forced to follow a specific path. When coupled with compression capabilities, PEP can also be used to reduce the amount of data that are inserted into the network [26].

Research is currently being conducted to combine PEP with an end-to-end security mechanism, such as IPSec. The problem associated with this implementation is that IPSec encrypts and/or authenticates the fields that the TCP PEP needs to be able to access. These include source and destination IP addresses as well as port and sequence numbers. A number of solutions, such as utilizing upper layer security mechanisms (SSL/TLS) instead of IPSec [2], placing the PEP before the IPSec protocol, coping hashed TCP flow control parameters in the new IP header [30] and encrypting different fields of the IP packet using different keys have been proposed [5].

B. SENSORS

Boost-phase intercept requires early launch detection and rapid, accurate tracking to launch and guide the interceptor. Although infrared or radar sensors can be used separately for initial detection and tracking, combining both approaches helps reduce the false alarm rate. Additionally, passive infrared sensors require triangulation from multiple sensors to obtain an accurate track because range information is not available [29]. For this purpose, forward deployable RF sensors could be used. Figure 2 illustrates these sensor options. Although detailed sensor architecture designs are quite complicated, their basic limitations and functionalities can be understood by examining the physics of each sensor type.

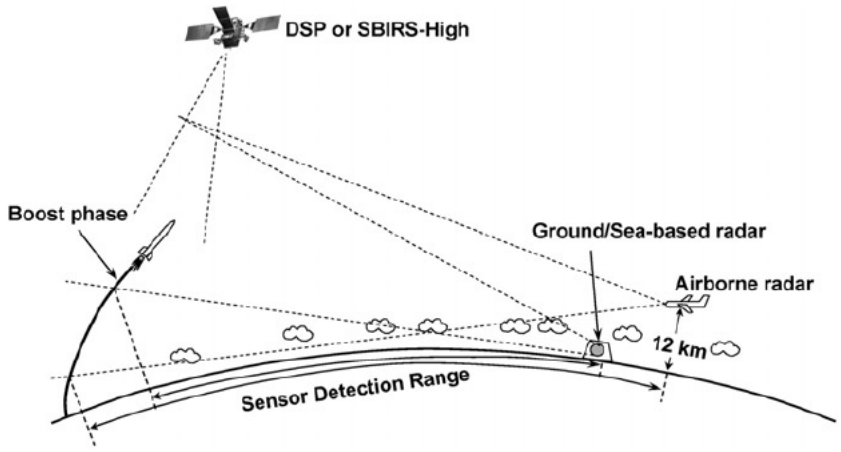


Figure 2. Sensor architecture schematic. Ground/Sea-Based and airborne RF sensors in combination with Satellite-Based IR sensors (From Ref. [29])

1. IR Sensors

Passive infrared systems can detect missile plumes from a distance of thousands of kilometers and, hence, can detect ballistic missile launches globally from high-Earth or geosynchronous orbits. Space-based IR sensors are very convenient because of their capability to cover wide areas. Infrared detection and tracking ranges depend on the infrared signal emitted by the target, the diameter of the optics, and the minimal detectable signal of the focal plane array, which is a function of the noise in the sensor and signal clutter returns from other objects (e.g., clouds, rain) in the sensor's field of view. Sensor noise is determined by the detector's dark current, which is a sensitive function of its operating temperature. The precision with which an infrared sensor can determine the missile booster position is determined by the pixel dimensions of the focal plane array [3].

The IR spectrum can be divided into four categories: (1) Short-Wave IR (SWIR) with wavelengths of 1-3 μm, (2) Medium-Wave IR (MWIR) with wavelengths of 3-5 μm, (3) Long-Wave IR (LWIR) with wavelengths of 8-12 μm and (4) Very Long-Wave IR (VLWIR) with wavelengths greater than 12 μm. Target emission obeys the blackbody radiation theory, initially derived by Plank in the early 1900s, in which the amount and wavelength (color) of the emitted radiation of a blackbody (ideal source of thermal radiation) are directly related to the temperature. This can be expressed as [3]

$$M(\lambda,T)=\frac{2\pi hc^2}{\lambda^5(e^{hc/\lambda \mathrm{KT}}-1)}\left[\frac{\mathrm{Watt}}{\mathrm{cm}^2\text{-}\mu\mathrm{m}}\right] \tag{2.2}$$

where $M(\lambda,T)$ is exitance of the object, λ is the wavelength, h is the Plank's constant, c the speed of light, T the temperature and K the Boltzmann's constant. Figure 3 is a plot of the blackbody radiation for different temperatures. The main idea is that as the temperature decreases, the peak of the blackbody radiation curve moves to lower intensities and longer wavelengths.

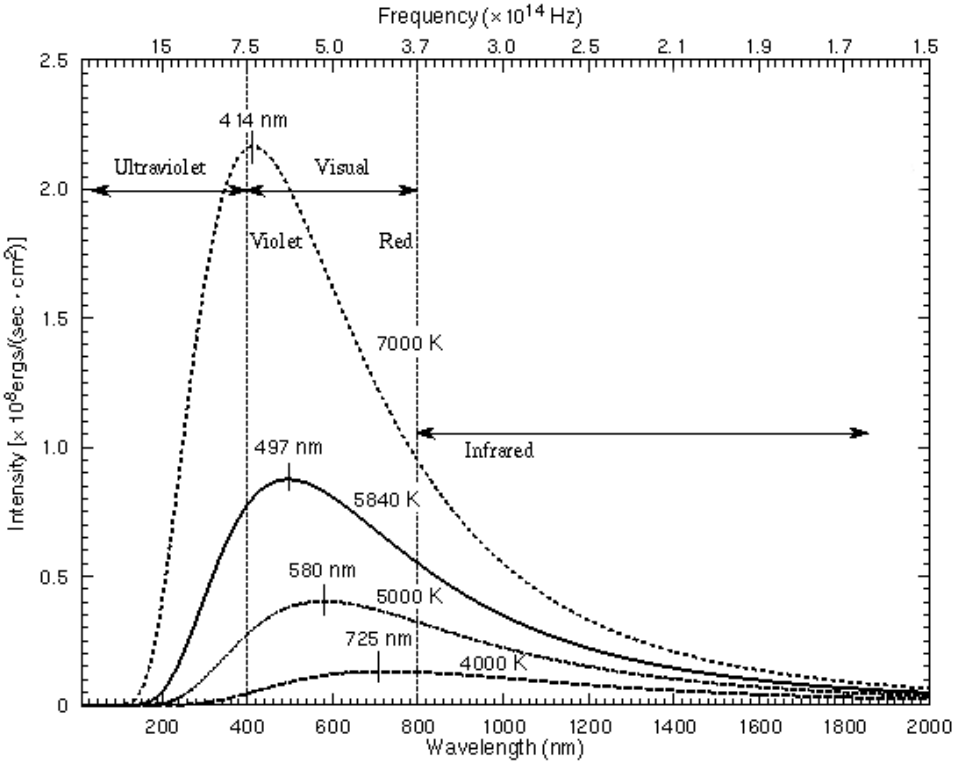


Figure 3. Blackbody radiation intensity for different temperatures (From Ref. [14])

a. IR Photo Detection

For the BMDS, detection of the missile should be performed either in the endo-atmosphere or exo-atmosphere. There are two critical differences with respect to detection and tracking in these two cases. IR sensors used at lower altitudes below atmosphere level (endo-atmosphere) observe and discriminate warm targets with high background irradiance from scattered sunlight in the Earth's surface. Exo-atmospheric IR sensors, on the other hand, engage targets that have cooler temperatures with low background irradiance levels because the space background has relatively much lower temperatures than the Earth's surface [25].

As derived from the blackbody radiation theory, a higher temperature target has a radiation peak at smaller wavelengths while at lower temperatures, longer wavelength emissions are generated. Applying these principles to the BMDS, it becomes

clear that IR sensors with multicolor capabilities should be deployed. Surveillance, target detection, and target tracking could be performed using single color sensors if the target is easy to identify. If either the target or the background is uncertain or dynamic during the engagement process, a sensor with multicolor capability will improve the probability of successful interception. Multicolor operation is essential at the point where the ICBM shifts from one phase of flight to another. The boost phase background is significantly different from that in midcourse, and, more importantly, the midcourse thermal signature is also substantially different since no plumes exist and proper discrimination from decoys and debris might be necessary [24].

Considering missile defense in both tactical and national theaters, IR sensors with multi-spectral (e.g., MWIR, LWIR, and VLWIR) as well as multicolor operation should be deployed. The sensors should exhibit high efficiency and uniformity. Along these lines, technology advancements are very promising in the field of Quantum Well Infrared Photo-detectors (QWIP), which play an important role in the sensing IR discipline [24].

b. Quantum Well Infrared Photo Detectors (QWIP)

The operation of conventional photo detectors is based on an inter-band transition of electrons across the band gap (E_g) between the valence and the conduction band as shown in Figure 4. Photons are used to excite the electrons resting in the valence band. Their energy (hv) must be sufficient to overcome the energy gap barrier; therefore,

$$hv > E_g \tag{2.3}$$

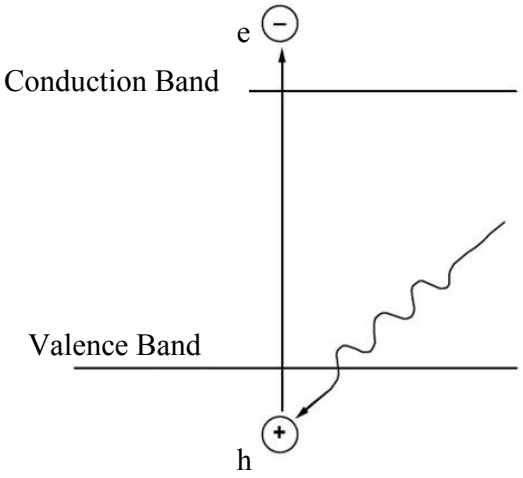


Figure 4. Band diagram of an intrinsic photo detector (From Ref. [7])

The photo-excited electrons can be collected to measure the produced photocurrent in a connected external circuit. This energy gap determines the spectral response of the photo detectors. Photosensitive materials have a defined energy gap, which constrains the photo detection to a single, limited band (one color photo detectors). Additionally, detection of VLWIR radiation up to 20 μm requires small band gaps down to 62 meV [7]. These low band gap materials are more difficult to grow and process than large band gap semiconductors, such as GaAs. Quantum Well Photo detectors (QWIP) offer the advantage of multiple band gaps and consequently expand the photo detector capability to multicolor. They are constructed by placing a thin narrow band gap material between wider layers of a wide band gap material. The idea of using QW structures to detect infrared radiation can be understood by examining the basic principles of quantum mechanics. The quantum well is equivalent to the well-known “particle in a box” problem in quantum mechanics, which can be solved by the time-independent Schrodinger equation. The solutions to this problem are the eigenvalues that describe energy levels inside the quantum well in which the particle is allowed to exist. The energy levels are primarily determined by the quantum well dimensions (height and width) [3]. Figure 5 illustrates a QW photo detector structure.

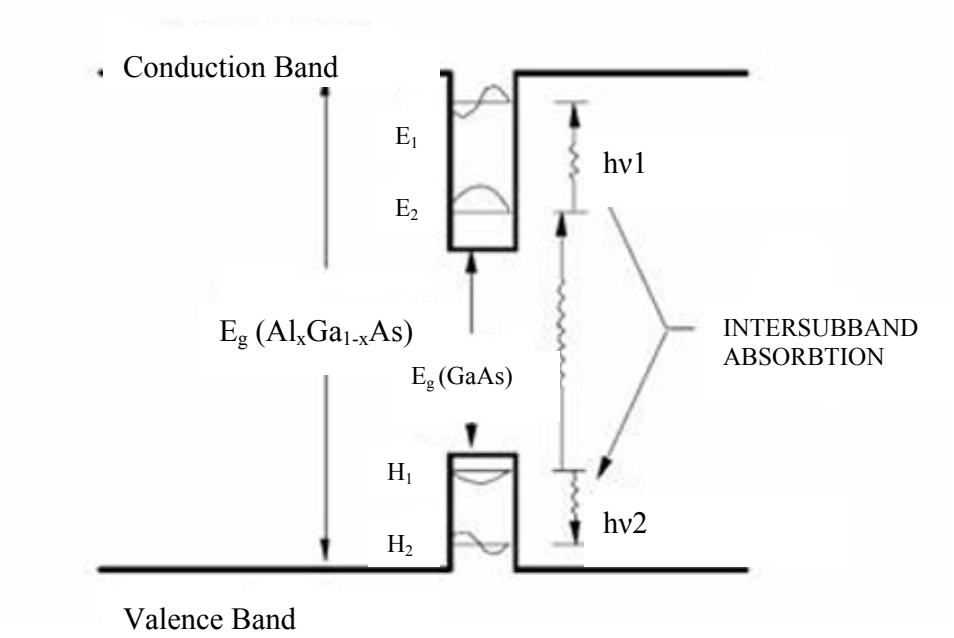


Figure 5. Quantum Well structure (From Ref. [7])

The position of the energy levels is determined by the thickness of the narrow band material and the band offset between the two materials. The QW structures offer the substantial advantage of having multiple wavelength detection capability (including the VLWIR band) in one sensor since different energy gaps exist. A common combination of materials used for QWIP is GaAs and AlGaAs due to their nearly identical lattice constants. A disadvantage of QW is its slightly lower operating temperature compared to detectors based on bulk semiconductors [24].

2. RF Sensors

Radars are a good means to provide accurate range measurements as well as efficient target tracking. Airborne radars, in particular, can provide early ballistic missile detection if the radar is approximately 400 km or less from the missile launch site because, at this range, an airborne radar flying at 12 km (40,000 ft) altitude has line of sight to the ground. Targets beyond this range must climb high enough to be seen over

the radar horizon [29]. If they are deployed inside the high risk area, they can provide the triangulation needed for the IR sensors to generate target distance and can valuably contribute to the boost phase interception of the missile.

Parameter	Ground-based X-band	Sea-based S-band	Airborne X-band
Operating Frequency (GHz)	9.5	3.3	10
Pulse repetition frequency (Hz)	45	17	30
Total average power (kW)	120	100	120
Antenna height (m)	2.0	3.85	2.0
Antenna width (m	4.6	3.65	4.0
Physical aperture (m2)	9.2	14.1	8.0
Effective aperture (m2)	6.0	2.0	5.2
Power aperture product (kWm^2)	720	1,200	624
Receiving gain (with weighting)	75,400	18,200	72,600
Weighted azimuth beam width (deg)	0.44	1.60	0.48
Weighted elevation beam width (deg)	1.01	1.52	0.96
Azimuth scan sector (deg)	90	90	90
Search solid angle (sr)	0.0278	0.0415	0.0264
Beam solid angle (sr)	1.36×10^{-4}	7.38×10^{-4}	1.41×10^{-4}
Noise temperature (◦K)	500	500	650
System and atmospheric losses (dB)	19.5	18.4	19.2

Table 3. Typical radar parameters (After Ref. [29])

Table 3 lists some of the typical characteristics of surveillance and tracking radar sensors that MDA uses for the BMDS (see also Table 1). In addition to the AEGIS Ballistic Missile Defense system (sea-based S-band radar) and the AN/TPY-2 (Terminal High Altitude Area Defense ground-based X-band Radar), MDA's plan for RF detection and tracking includes the new Sea-based X-band radar (SBX). SBX is a floating, self-propelled radar, platform, capable of operating under heavy weather conditions and exhibiting robust discrimination capabilities.

C. SECURITY

The dynamic topology and wireless nature of the hybrid networks associated with strategic missile defense scenarios drive the requirement for a fail-safe node and data authentication scheme and robust data confidentiality mechanisms. As these scenarios

evolve in both time and space, new elements are often introduced into the existing network. The sensitivity and importance of the data being exchanged within the network often leaves no room for revealing all, or even part, of the information to an untrusted node. The primary requirement, therefore, becomes the effectiveness of the security mechanism in providing data encryption and node and data authentication, even at the price of longer delays. That being said, the real-time bounds still apply as there is clearly a limit on the useful lifetime of the sensed data.

Data confidentiality can be achieved through encryption using symmetric and asymmetric cryptographic algorithms. Larger key lengths increase the strength of the algorithm but lead to longer decryption and encryption delays.

Although minimizing network delays whenever possible is an important design objective, the initial node authentication scheme can tolerate increased latency. This is because prior to node authentication, new nodes are not active members of the network and do not share the same real-time data delivery requirements of nodes already in the network. In contrast, data authentication clearly requires a bounded minimum delay, particularly among nodes exchanging sensor data within the AOI for target tracking. Additionally, this target information must be aggregated and transmitted back to the command and control node in a timely fashion to meet stringent decision timelines and potential weapon assignment requirements. To guarantee authenticity of the transmitted data, the data must be verified that each packet originated from a valid (authenticated) source and that it was not altered during transit. Accordingly, the data authentication protocol should minimize end-to-end latency of the data packets and demonstrate robustness in the face of packet losses. Low per-packet overhead will also increase data throughput and minimize the authentication computation time.

The security mechanism proposed in this thesis is designed to meet the requirements identified above. Although this thesis focuses specifically on authentication and confidentiality of the transmitted data, there are a number of other security challenges that must also be addressed in a complete security solution. Many of these can be adapted directly from existing work in both WSN and MANET research and include such issues as defending against denial of service (DoS) attacks, detecting misbehaving nodes,

avoiding eavesdropping of traffic, preventing traffic analysis, and key management issues. This section provides a brief overview of the security primitives that will form the foundation of the proposed authentication and confidentiality schemes.

1. Symmetric Ciphers

Symmetric ciphers use the same secret key for both the encryption and the decryption processes. These processes consist of four components:

- The original message.
- The encryption/decryption algorithm that performs all the necessary transformations on the input message.
- A secret key that is fed in as an input to the algorithm along with the original message. This key is responsible for scrambling the message during encryption or producing the original message during decryption.
- The output of the process, known as the cipher text.

Symmetric encryption depends on the secrecy of the key used for the encryption and not on the secrecy of the algorithm used. An attacker with prior knowledge of the algorithm and one or more cipher texts should not be able to extract the cipher key or, of course, read the original message. A number of symmetric ciphers have been proposed with various key lengths. The larger the key, the stronger the encryption is. Examples of symmetric ciphers include Digital Encryption Standard, DES (Federal Information Processing Standards, FIPS PUB 46-2), 3DES (National Institute of Standards and Technology, NIST, Special PUB 800-67), Advanced Encryption Standard, AES (FIPS PUB 197) and Rivest Cipher, RC4. Primary differences among these schemes are the key length used (some support variable key lengths), the performance time, and the way in which they process the plain text. A stream cipher processes the original message as one continuous input whereas a block cipher first breaks the original message into blocks and then produces a distinct output for each input block.

a. Block Ciphers and Modes of Operation

Most block ciphers break up messages into blocks of 64 bits and chain them together after the encryption or the decryption. Four common chaining mechanisms exist [21]:

(1) Electronic Codebook (ECB). This chaining mechanism encodes each block independently but uses the same key. Thus, the same plain text will always result in the same cipher text. It is generally not considered very secure because it is susceptible to pattern matching, a common technique used by crypto analysts.

(2) Cipher Block Chaining (CBC). In CBC, the current block is XORed with the previous block. An encrypted block of random data, called the initialization vector (IV), begins the chaining process and is XORed with the first message block. Figure 6 illustrates the CBC mechanism.

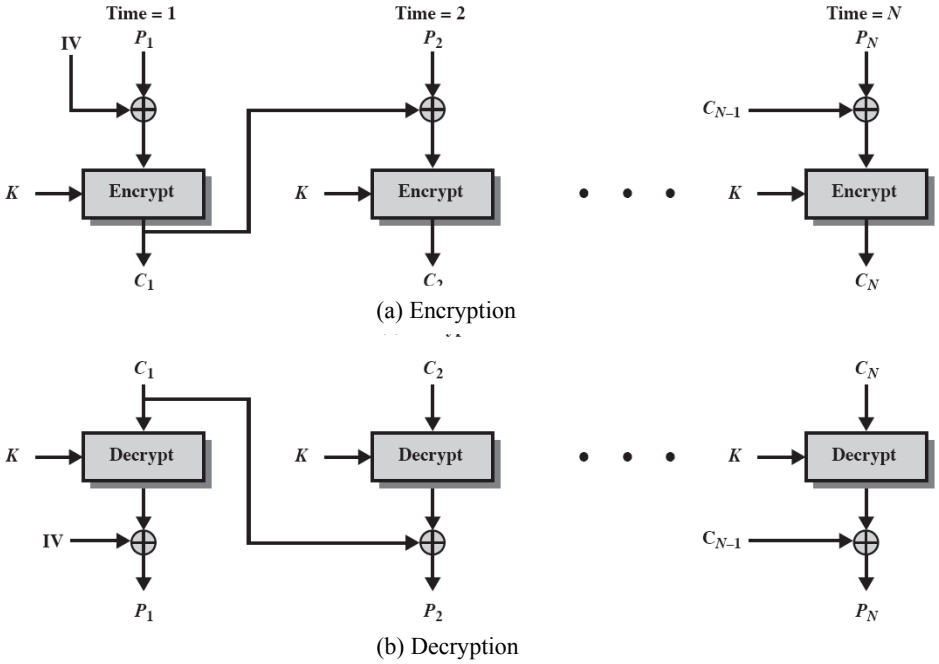


Figure 6. Cipher Block Chaining (CBC) Mode (From Ref. [23])

(3) Cipher Feedback Mode (CFB). Similar to the CBC. The only difference is that CBC uses the cipher text of the preceding block rather than the plain text.

(4) Output Feedback (OFB). A variation of the CFB mode in which the XORed block is randomly generated and is, therefore, independent of the preceding plain text.

b. Stream Ciphers

A stream cipher processes the input plaintext as a single message, producing the scrambled output in byte or even bit intervals as it executes. The key is fed as input into a pseudorandom byte generator, and the resulting key stream is XORed byte-wise with the plaintext, producing the desired encrypted output. Decryption is performed in the reverse order. Figure 7 presents the stream cipher operation.

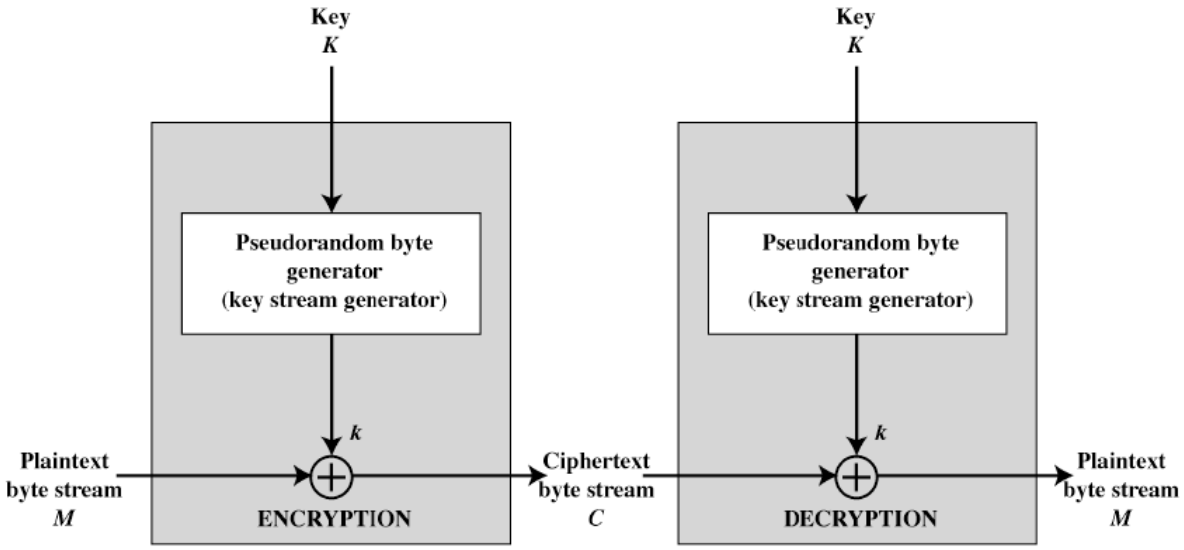


Figure 7. Stream Cipher Operation (From Ref. [23])

The primary advantage of stream ciphers over block ciphers is that they are faster and simpler to implement. The major disadvantage is that if the pseudorandom generator is poorly designed, it will eventually repeat itself and make the secret key subject to compromise.

2. Public Key Cryptography and RSA

In asymmetric encryption, two different but mathematically related key values are required: a public key and a private key. With these keys, if the plaintext is encrypted using the public key, it can only be decrypted using the private key (and vice versa). The private key is kept secret while the associated public key is readily available and publicly distributed hence the name "public key cryptography."

a. Principles of Public Key Cryptosystems

To understand the advantages of the asymmetric system, consider two people who would like to communicate secretly over a public (and shared) medium. With the symmetric approach, these two people would have to share the same secret key. With the asymmetric approach, the sender encrypts the message with his private key and the recipient uses the associated sender's public key to perform the decryption. The obvious advantage is that the sender does not have to transmit the key used for the encryption (in our case, his private key) to the receiver. This reduces the probability that a malicious third party can spoof the key and compromise the network message traffic.

Applications that use public key cryptosystems can be broadly arranged into three categories [23]:

(1) Encryption/Decryption. The recipient's public key is used by the sender for encryption.

(2) Digital Signatures. The sender uses his private key to digitally sign the original message. The recipient decrypts the message with the sender's public key.

(3) Key Exchange. A temporary key used for during a single session is distributed by encrypting it with the private key of either the sender or the receiver.

Asymmetric algorithms are designed so that the key for encryption is different from the key for decryption. The decryption key cannot be calculated from the encryption key (not in any reasonable amount of time) and vice versa. The usual key size ranges from 512 to 2048 bits [21]. These algorithms are relatively slow compared to symmetric ones and their design is based on computational problems, such as factoring extremely large numbers or computing logarithms of extremely large numbers. Diffie-Hellman [4], Digital Signature Standard (DSS) [FIPS 186], Rivest-Shamir-Adelman (RSA) [20], and Elliptic-Curve cryptography [10] are examples of asymmetric algorithms. In the next section, we will briefly discuss the RSA algorithm because part of our proposed node authentication scheme is based on this asymmetric algorithm.

b. The RSA Algorithm

Most of the asymmetric algorithms are based on modular arithmetic. According to [STALL06], "Modular arithmetic is a kind of integer arithmetic that reduces all numbers to one of a fixed set [0…n-1] for some number *n*. Any integer outside this range is reduced to one in this range by taking the remainder after division by *n*." Analyzing modular arithmetic is beyond the scope of this thesis, but the definition will help the reader to understand the basic concepts behind the RSA algorithm.

The RSA algorithm [20] was initially proposed in 1977. With the patent expiration in 2000, the algorithm has since become available to the public. Compared to similar algorithms, it is easier to understand and implement. It has undergone many years of extensive cryptanalysis. It is flexible and can accommodate variable key lengths (usually ranging from 512 to 2048 bits). RSA's security mechanism is based on the difficulty of factoring very large numbers. RSA keys are generated as follows:

(1) Select two large prime numbers p and q.

(2) Compute: $n = p \times q$

(3) Chose an extremely large prime number *e,* with the constraint that *e* and (*p-1*)(*q-1*) are relatively prime. The public key is then the concatenation of *e* and *n* to form (*e, n*).

(4) Calculate the private key *d* such that

$$e \times d = \text{mod}(p-1) \times (q-1) \qquad (1.3)$$

$$d = e^{-1} \text{mod}(p-1) \times (q-1) \qquad (1.4)$$

Upon calculation of *d*, the numbers *p* and *q* are no longer needed and can be discarded but must not be revealed.

3. Message Authentication and Hash Functions

Encryption provides a means to protect against eavesdropping and spoofing, but it is also necessary to ensure that the received message originated from a valid source and was not altered during transit. Additionally, any authentication method utilizing timestamps can also verify that the message has not been replayed or delayed longer than anticipated. The three most common message authentication schemes are: conventional encryption, hash functions, and message authentication codes (MAC) [23]. In the following sections, we will briefly discuss each of these three major authentication approaches.

a. Conventional Encryption

Conventional encryption is a relatively simple principle and is based on shared knowledge of a single secret key held by both the communicating entities. The sender encrypts the message using the secret key and transmits only the cipher text. The recipient decrypts the received cipher text, using the same secret key. Authentication is also achieved since the sender and receiver have knowledge of the key. It is critical that the secret key is not comprised. This method works well for point-to-point communication but requires a node to maintain a copy of the secret key for all potential communication partners. Key management problems arise when the communication is expanded to multiple nodes. Solutions to this multiple node problem have been proposed that use hash functions and message authentication codes [23].

b. Hash Functions

A hash function takes an input message of arbitrary length and produces a fixed-length output. The hash output is called the message digest. The hash algorithm is cryptographically secure if it demonstrates the following properties [23]:

(1) The same input always produces the same output.

(2) It should be computationally infeasible to find two messages that produce the same digest.

(3) It should be computationally infeasible to produce the input message given the output (i.e., it is a one-way function).

Hash functions provide data integrity and are commonly used to generate a fingerprint of a message or a file. Because a hash digest of a message is unique, it provides both integrity and authenticity. Hash digests of messages are usually appended to and transmitted with the original messages. The recipient receives both the message and the hash of the message. It computes the hash (the algorithm used is known) and compares the two hashes. If they match, it is assumed that the message has not been altered.

Several hashing algorithms have been proposed in the literature. Examples include MD5 (RFC 1321), SHA-1, SHA-256, SHA-512 (RFC 3174), and others. The primary difference among them is the output size. For example, MD5 produces a 128-bit output where SHA-256 produces a 256-bit output (as shown in Table 4). Notice, however, that if hash functions are not combined with any other authentication protocols, they guarantee the message's integrity, but not the sender's authenticity.

	SHA-160	**SHA-256**	**SHA-384**	**SHA-512**
Message digest size	160	256	384	512
Message size	Less than 264	Less than 264	Less than 2128	Less than 2128
Block size	512	512	1024	1024

Table 4. Comparison of SHA parameters (After Ref. [23])

c. Message Authentication Codes and HMAC

The message authentication codes (MAC) technique is similar to a hash function in that it uses a secret key to generate an authentication code, which is appended to the original message. Upon message reception, the MAC is recalculated (both nodes again share the same secret key) and the two MACs are compared. If they match, the message has not been altered. Figure 8 presents the MAC algorithm operation.

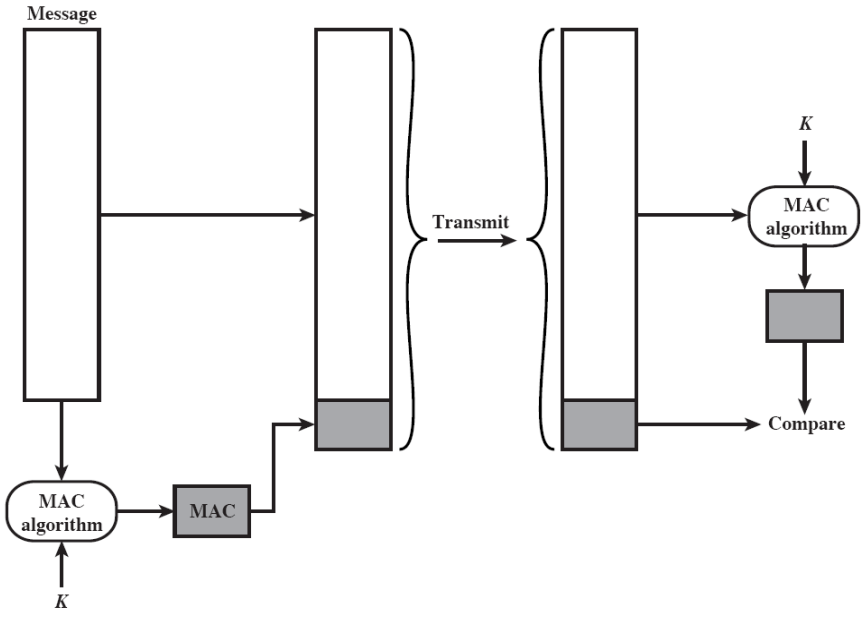


Figure 8. Message authentication using MAC (From Ref. [23])

In FIPS PUB 113, the National Institute of Standards and Technology (NIST) recommends the use of Data Encryption Standard (DES) for the MAC calculation. There was an increased interest in the industry for developing a hash-based MAC because hash functions are readily available in the public domain (unlike conventional cryptographic algorithms, which are typically patented) and hash functions operate faster. The end result was RFC 2104, which defined HMAC (Hash-MAC) for secure Internet protocols.

4. Digital Signatures

A digital signature is an encrypted message digest that is appended to a message. Digital signatures are based on a combination of public key encryption as well as secure hash function and confirm both the sender's identity and the integrity of the message. They rely on public key cryptography in that they require the sender to own both a unique private and a public key. The process of digitally signed messages includes the following steps:

(1) The sender creates a private/public key pair.

(2) The sender transmits the public key to the receiver.

(3) The message is hashed and the message digest is produced.

(4) The message digest is encrypted with the sender's private key.

(5) The digital signature is the encrypted hash. A copy of the original message and the digital signature is transmitted to the receiver.

In order to verify the signature, the receiver:

(1) separates the message from the digital signature,

(2) applies the sender's public key to decrypt the message digest,

(3) takes the original message and feeds it into the same hash function, and

(4) compares the two outputs to see whether they match.

Although digital signatures authenticate both the sending node identity and the integrity of the message, they do not provide data confidentiality. Separate confidentiality mechanisms can be applied in parallel to ensure both confidentiality and integrity.

Digital signatures are susceptible to spoofing as can be seen by the following example. Consider an adversary who sends his public key to the receiver, pretending that this public key belongs to a legitimate sender. The adversary can now digitally sign messages with his private key and the receiver will assume that they originated from a trusted sender because the messages would decrypt correctly. Public key infrastructure (PKI) can be used to provide a solution to this problem.

PKI is based on a trusted third party, called the certificate authority (CA) who is responsible for creation and distribution of certificates. A certificate contains a user ID, the public key for that user, and the CA's digital signature. PKI assumes that the CA is a trusted node and that its private keys are not subject to compromise.

5. IPSec

There exist a number of application-specific security mechanisms that provide confidentiality, authenticity, and integrity. IPSec was designed to be transparent to the application layer and is a collection of RFCs that provide mechanisms, protocols and message formats to achieve secure point-to-point confidentiality and integrity at the IP layer.

a. IPSec Architecture

IPSec offers a number of security services including access control, integrity, authentication, anti-replay, and confidentiality. When IPSec is applied in a point-to-point communication system, nodes on both ends of the communication link are required to agree on a pre-defined set of security parameters. In the following sections, the protocols, formats, and mechanisms used by IPSec are briefly explained. Table 5 provides a summary of the IPSec framework's services and underlying mechanisms.

Services	Mechanism
Confidentiality	Encryption, ESP Header, ESP Packet
Integrity	Originator authenticity
	Anti replay, Sequence number in ESP header
	Data integrity, Integrity check value (ICV)
Authentication	Authentication header (AH)
Key management	Internet key exchange (IKE)

Table 5. Summary of the IPSec services (After Ref. [21])

b. Authentication Header (AH)

AH is used when only authentication and not confidentiality is required. It provides data authentication and integrity for IP packets between the two systems, but it does not encrypt the data packet. Authentication is achieved through the use of a HMAC. The two entities share a secret key, a message digest is produced, and the digest is appended as an AH header to the data. The receiver compares the digests to verify the integrity of the message. Because HMAC uses a symmetric key, the authenticity of the packet is guaranteed. AH supports various types of HMACs. Figure 9 shows the AH appended to an IP packet.

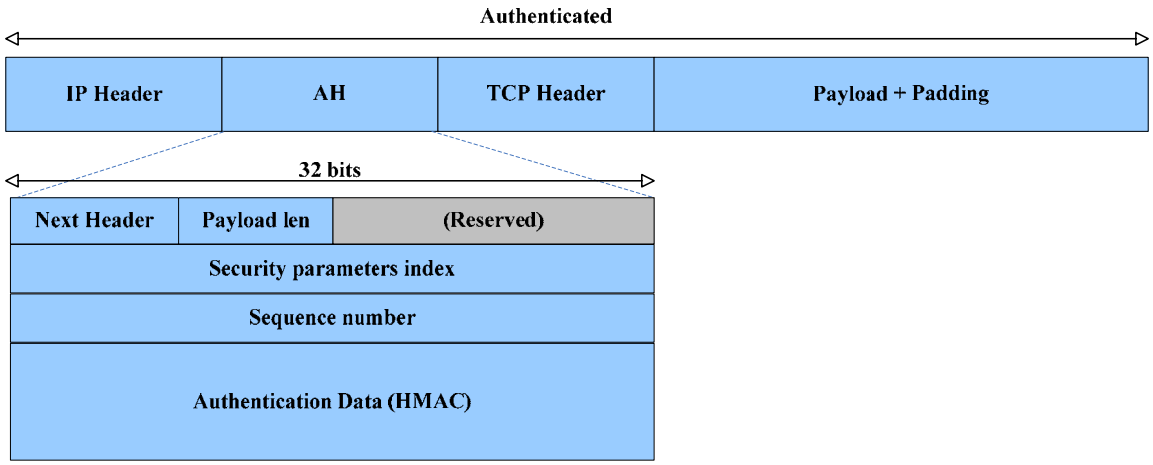


Figure 9. Authentication Header appended to an IP packet (AH)

The Authentication data field holds the integrity check value (ICV), which is a truncated MAC code. It has a length of 96 bits and is calculated over the TCP header and upper layer data, the AH, and the fields of the IP Header that do not change during multi-hop transmission.

c. Encapsulating Security Payload (ESP)

ESP is used when encryption is needed. ESP can also provide optional authentication for the IP packet payload, and the ESP header. It provides confidentiality by encrypting mainly payload, and it supports several symmetric encryption algorithms,

such as DES, 3DES, and AES. When it is used with the authentication option, the encrypted IP datagram and the ESP header and trailer are included in the hashing process. A new IP header is appended in front of the packet for routing purposes. Figure 10 shows the ESP format.

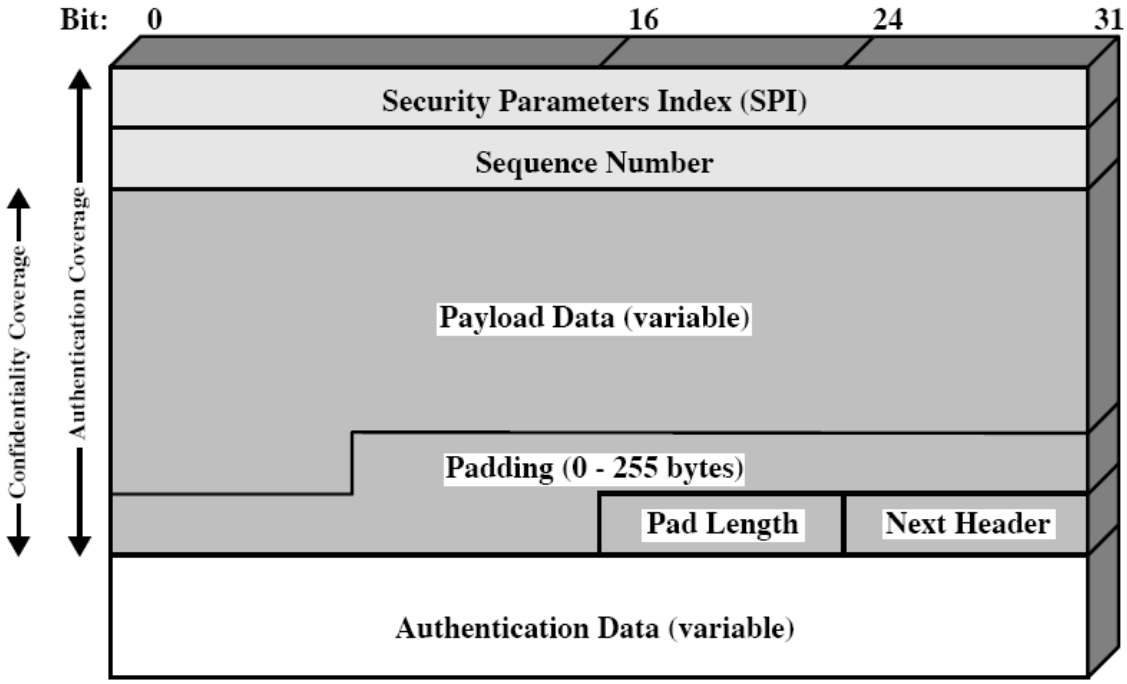


Figure 10. Encapsulating security payload (ESP) format (From Ref. [23])

d. Modes of Operation

Both AH and ESP can be applied to IP packets in two different modes: Transport and Tunnel mode.

(1) Transport Mode. Transport mode is primarily used for end-to-end transmissions between hosts. It protects the payload of the packet but leaves the original IP address unencrypted. The original IP header is used for routing purposes. Accordingly, transport mode provides security to the higher layer protocols only.

(2) Tunnel Mode. In this mode of operation, a new IP header is inserted after the original IP header. This mode protects both the payload and the old IP header.

Figures 11 and 12 illustrate how transport and tunnel modes are implemented with both AH and ESP.

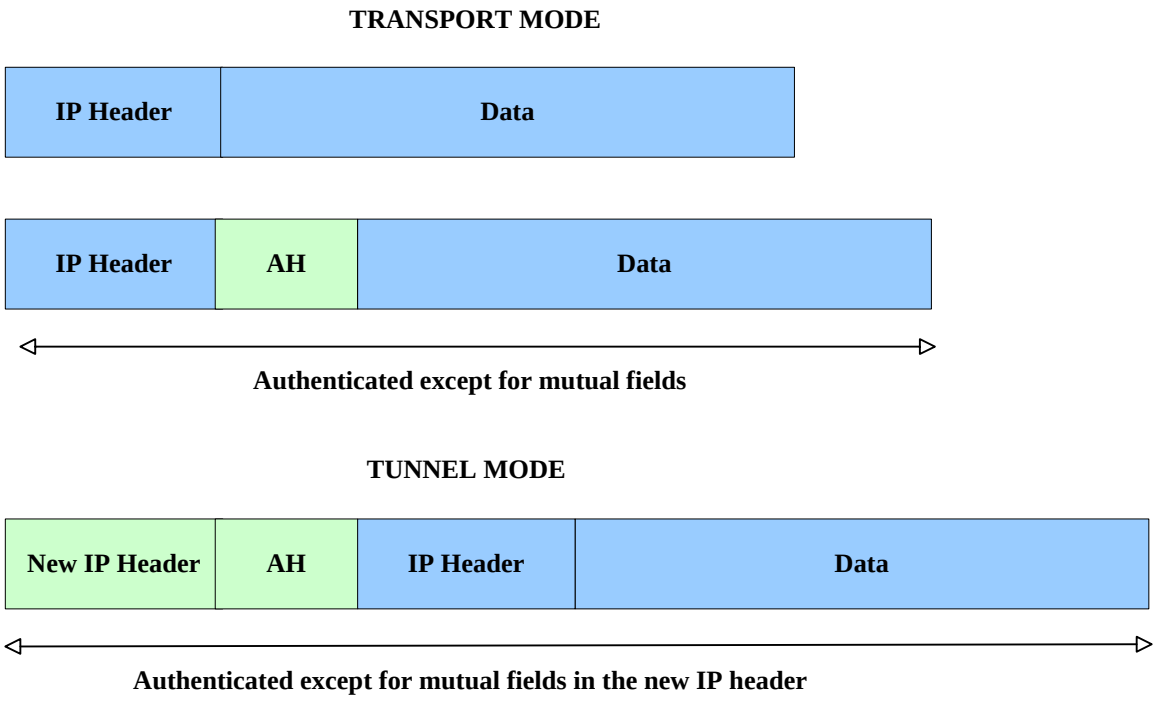


Figure 11. AH transport and tunnel mode

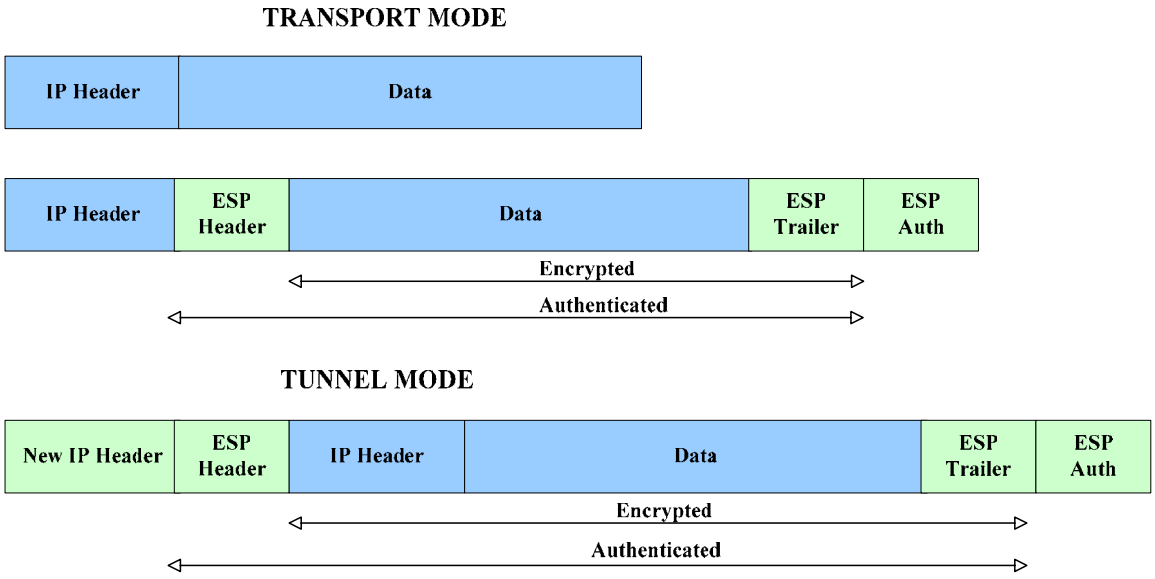


Figure 12. ESP transport and tunnel mode

e. Security Associations (SA)

The concept of a security association (SA) is fundamental to the IPSec implementation. A SA is an agreement between two communicating entities on how the IPSec security services will be used. A SA includes the encryption and authentication algorithm as well as the session shared key. This key will be used in all the functions of the IPSec framework that require the use of such a key (e.g., the HMAC). Different SAs can be used for each communication direction to protect the traffic stream. Every SA is uniquely identified by a number called the security parameter index (SPI) and the destination IP. When a system wants to send a packet protected by IPSec, it chooses the desired SA, processes it accordingly, and inserts the proper SPI into the IPSec header. The receiver follows exactly the same procedure.

f. Key Management

IPSec supports both manual and automatic distribution of keys. Manual key management requires an administrator to manually configure each system with the keying material and the SA parameters and is not preferred in large implementations. Clearly, this option does not scale efficiently. The default automated key management

protocol selected for IPSec is the Internet Security Association and Key Management Protocol (ISAKMP), sometimes referred to simply as Internet Key Exchange (IKE). ISAKMP defines procedures and packet formats for the SA and payloads during the key exchange and distribution. A more detailed description of ISAKMP can be found in RFC 2408.

D. SUMMARY

This chapter examined the topology and architecture of a hybrid, large-scale network for ballistic missile defense and identified an accompanying set of real-time data dissemination requirements and satellite link constraints. An overview of the IR and RF sensors was provided, with an emphasis on the QWIR IR sensors. Security issues regarding node and data authentication were addressed, and the important role of data confidentiality was highlighted.

The chapter closed with an overview of the security primitives and protocols used in the proposed multistage authentication and confidentiality scheme that follows. Detailed descriptions can be found in the corresponding RFCs.

THIS PAGE INTENTIONALLY LEFT BLANK

III. PROPOSED MULTISTAGE AUTHENTICATION AND CONFIDENTIALITY SCHEME

This chapter describes a multistage security mechanism that provides node and data authentication as well as data confidentiality. A two-stage node authentication scheme ensures that only a node with legitimate credentials will join the network, participating in the target data exchange while the Timed Efficient Stream Loss-tolerant Authentication (TESLA) algorithm combined with strong encryption in the network layer guarantees that the data were not altered, that they originated from a trusted source, and that there were not comprised by an unauthorized adversary.

The result is an efficient and effective multistage scheme that accommodates the requirements and constraints identified in Chapter II. To simplify the discussion, the notation in Table 6 is used to describe the cryptographic protocols and operations in this thesis.

N	Node requesting access to the network
A	Authenticator, a node that protects and controls access to the network verifying the credentials presented
ID	Node's identification code
K	Encryption key shared or derived
Enc(M,K)	Encryption of message M using key K
Dec(M,K)	Decryption of message M using key K
N-Pub, N-Pri	Node's public and private key pair
A-Pub, A-Pri	Authenticator's public and private key pair
H(M)	Hashed output of message M.

Table 6. Notation used to describe the operation of the proposed multi-stage solution (From Ref. [9])

Additionally, the following assumptions are made:

- The command and control node is considered to be a trusted source.
- All the nodes within the network can communicate with the command and control node. (Note that this may be multi-hop).
- Private keys are not compromised.

- Nodes are not constrained by processing or energy limitations; therefore, the encryption keys will be chosen with the maximum security criterion.

A. DATA CONFIDENTIALITY

In our proposed security scheme, the data confidentiality function is performed entirely by IPSec. IPSec is applied at the IP layer and is not application specific. This provides flexibility and scalability and allows our scheme to support any future application properly configured for secure data dissemination. We propose ESP packets in the transport mode. ESP is preferred over AH because our primary objective is confidentiality rather than pure authentication. The transport mode is preferable to the tunnel mode because real-time data dissemination requires minimization of the authentication delay. In tunnel mode, additional delay would be added without significant gain.

B. NODE AUTHENTICATION

The two-stage node authentication scheme is comprised of a centralized phase followed by a distributed phase.

1. Centralized Authentication

Initially, a centralized approach is used in which the command and control node (acting as the central authenticator) grants or denies access based on credentials presented by the joining node. The centralized authentication flowchart is presented in Figure 13.

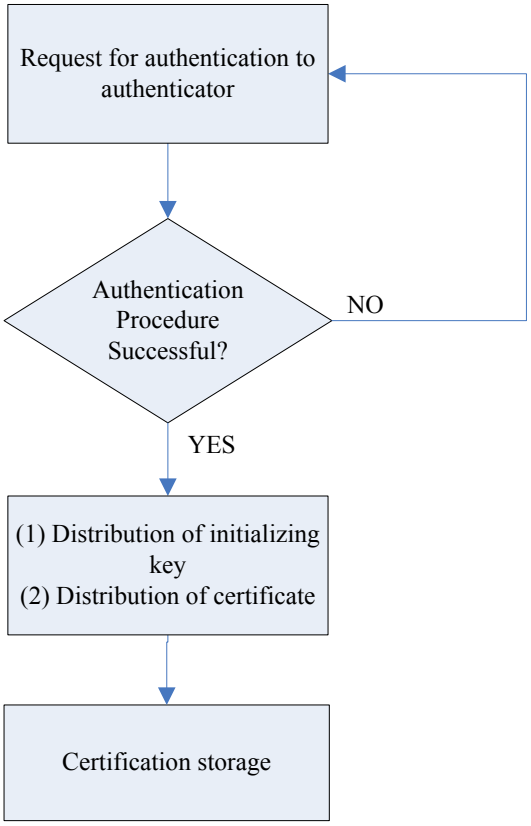


Figure 13. Centralized node authentication

The scheme is initiated when the joining node issues a request for authentication to the command and control node. The pseudocode of the algorithm is presented in Figure 14. A valid node ID is a significant piece of information for an adversary who may want to break into the network. It is, therefore, imperative that the node ID is not transmitted unencrypted. Additionally, the use of the digital signature in Step 1 ensures that the hashed output of the node ID is sent only by the supplicant node. The ID and the key used to encrypt this ID will be utilized by the command and control node as authentication verification.

```
\BEGIN
        ID is hashed: H(ID)\\
        Encryption of the hash with N-pri: Enc(H(ID), N-pri)\\
        Generation of a random key K\\
        Encryption of ID with K: Enc(ID,K)\\
        Encryption of K with A-pub: Enc(K, A-pub)\\
        Transmission of Enc(H(ID), N-pri), Enc(ID, K),  Enc(K, A-
    pub)\\
\END
```

Figure 14. Pseudocode of centralized authentication phase request

The command and control node receives the authentication request and completes the algorithm outlined in Figure 15. The decrypted node ID is used to determine which public key pair should be applied for the decryption of the hashed ID value (it is encrypted with the node's private key). The authenticator must maintain a table that associates node IDs to public keys. This table will include a full list of valid nodes for the given network. In the scenarios envisioned, these nodes could be land-based stations, warships, aircraft, and unmanned air vehicles (UAV) or satellites. A predefined time schedule could be used to renew valid nodes' IDs in the table. In addition to providing a mechanism to support dynamic updates, this can also be used to reassign node IDs in the event that a node ID is compromised.

```
\BEGIN
        Decryption of Enc(K, A-pub) with A-pri\\
         Decryption of Enc(ID,K)with K \\
         Decryption of Enc(H(ID), N-pri) with N-pub\\
         ID is hashed H`(ID)\\
       If H`(ID)=H(ID)
         N is authenticated
       else
         N is denied access\\
\END
```

Figure 15. Pseudocode of centralized authentication phase response

The authenticator selects the appropriate public key and decrypts the hashed ID. At this point, the authenticator knows both the transmitted node ID and its transmitted hashed value. The authenticator then internally produces the correct hash of the provided ID and compares the two hashes. If they match, the node is authenticated successfully. The command and control node informs the other network nodes that a new node has been granted access by issuing a certificate, which includes the node's current ID and its public key. This certificate is distributed to all active nodes and will be used during the distributed node authentication phase. The authenticator also distributes an initializing key to the new node which will be used to generate a set of keys for subsequent data authentication.

2. Distributed Authentication

In the distributed node authentication phase, the joining node is authenticated by the active network nodes. This phase is presented in Figure 16. To support routing functionality, the new node should be authenticated by all of its one-hop neighbor nodes.

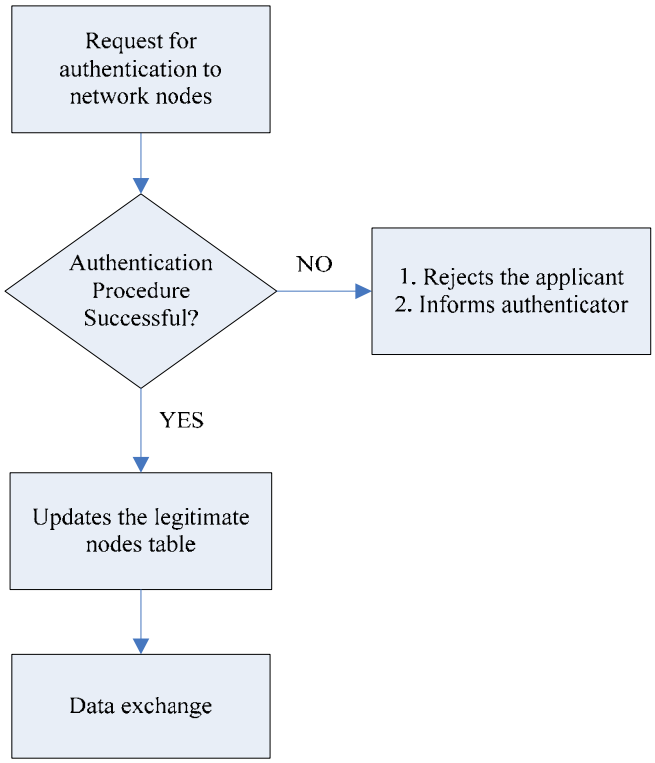


Figure 16. Distributed node authentication

All active nodes maintain a table of all other active nodes in the network. This table contains node IDs, corresponding public keys, and a flag indicating whether the indexed node has passed the distributed authentication procedure. Only distributively authenticated nodes can participate in a data exchange with this node. This table is updated when a certification is received and when a node completes the distributed part of the authentication procedure.

All active nodes receive the certificate that the command and control node issued for the new node. The message exchange procedure outlined in the previous section is initiated and repeated for each neighbor node because the neighbor nodes are now aware of the new node's ID and public key. Once the authentication procedure succeeds, the table at each neighbor node is updated and the new node is permitted to engage in data exchange.

C. DATA AUTHENTICATION

In our scheme, the Timed Efficient Stream Loss-tolerant Authentication (TESLA) protocol is chosen for data authentication because it provides low per-packet overhead, small authentication delay, and robustness in the face of packet loss. This protocol is described in detail in [15], but we provide an overview in the following paragraphs.

TESLA assumes all the nodes are "loosely time synchronized." By "loosely time synchronized," we mean that the receiver should be aware of a maximum value for the synchronization error that is calculated during the setup phase.

To send an authenticated packet, the sender computes a MAC for the packet with an undisclosed key. The key used for this MAC will be disclosed in future packets according to a predefined key disclosure schedule. When the receiving nodes get the packet, they can verify that the MAC key has not yet been revealed (they are loosely synchronized) and that the total delay (transmission and propagation) of the packet is within expected limits. If these conditions are met, the packet is buffered. After the key disclosure interval passes, the receiver receives the key used for the MAC for the buffered packet, and, if the key is correct, the packet's authenticity is verified.

During the setup phase, the sender generates a set of keys utilizing a pseudorandom function. These keys will be used for the generation of the MAC keys and are generated using a key chain. This means that each generated key is used as an input for the generation of the next key of the chain

$$K_{i+1} = H(K_i). \tag{3.1}$$

The sender picks the last key in the sequence and uses it as an input to another hash function to produce the first MAC key for the first authenticated packet. Because H is a one-way function, any node can compute forward keys but not backward keys.

At this point, the sender has generated two sequences of keys. The first key chain $K_{i...n}$ is used in the reverse order for the generation of the second key sequence (i.e., the MAC keys). A logical implementation would associate the number of the keys produced with the number of the transmitted packets. To achieve faster transmission rates, the algorithm associates keys not directly to packets but to time intervals. The packets that are transmitted within a specific time interval are all authenticated with the same MAC key.

Every packet transmitted contains the following: the data payload (the message), the hashed value of the key used to compute the MAC of the following packet, and the original key used for the MAC of the previous packets (how far back depends on the key disclosure time). In Figure 17, we assume that the receiver has received and authenticated packets P_1 and P_2 and it receives packet P_3. P_3 contains both K_1, and $H(K_3)$, as well as the data itself. The receiver has already received $H(K_1)$ from previous packets. It has also received K_1 but has yet to verify that the key is valid. It calculates the digest of K_1, and, if the two hashes match, the key is authentic and it can verify packets P_1 and P_2. It has already received $H(K_3)$, but it cannot authenticate P_3 because it has not yet received K_2. It buffers P_3 and waits for the reception of the next group of packets. When P_4 and P_5 are received, the receiver performs the same procedure for the authenticity of P_3 since P_4 contains K_2. It calculates the digest of K_2 and compares the hashes. The procedure continues until the end of the transmission.

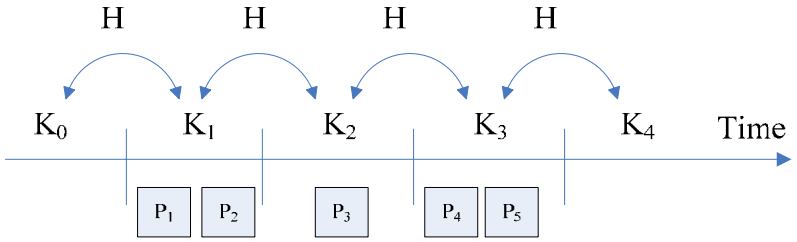


Figure 17. TESLA Authentication algorithm example

The receiver utilizes a time-out mechanism to drop packets whose delay exceeds a pre-determined bound that is included to minimize the ability of an adversary to forge packets in the case of a compromised key disclosure schedule. As mentioned earlier, this protocol requires loose time synchronization between the sender and the receiver. Whenever a key is received, the following security condition has to be met:

$$d = \left\lceil \frac{t_{\max\_sync\_err} + t_{\max\_delay}}{t_{\text{int}}} \right\rceil \tag{3.2}$$

where $t_{max\_sync\_err}$ is the maximum synchronization error between the sender and the receiver, t_{max_delay} is the maximum one way network propagation delay and t_{int} is the time interval defined by the sender. Larger values of d increase the authentication time because the receiver will have to buffer all the received packets until the appropriate authentication key is received.

It is desirable to minimize d to improve the real-time dissemination performance. TESLA accommodates variable packet flow rates by determining d for each chain. Multiple chains allow the binding of links with different channel characteristics (e.g., propagation delay and transmission rate).

In our scheme, the initializing key used to produce the key chain is distributed to the new node by the trusted command and control node during the centralized authentication phase as shown in Figure 13. As we shall see in Chapter IV, this parameter manages the trade-off between the level of security and the authentication delay.

D. SUMMARY

The proposed multistage security mechanism for a hybrid, large-scale network for ballistic missile defense has been presented. The importance of a multistage node authentication was addressed, and an algorithm that meets this requirement was proposed. It is the based on public key infrastructure and digital signatures for node authentication. The TESLA algorithm, a proposed Internet standard, is the protocol of choice for the real-time data authentication. Among other features, it exhibits robustness in the face of packet losses and accommodates variable data rates. Data encryption is provided by IPSec. The choice of encryption at the IP layer provides the advantage of flexibility and application independence.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. PERFORMANCE ANALYSIS AND SIMULATION

The performance analysis and simulation of the proposed multistage authentication and confidentiality scheme can be divided into two parts. The first part focuses on the authentication while the second part focuses on the confidentiality. The authentication analysis examines both the node and data authentication delay. The confidentiality results compare total delay associated with IPSec to that of unencrypted IP.

A. NODE AND DATA AUTHENTICATION

This section provides performance analysis as well as simulation results for both the node and the data authentication mechanisms. Data packets cannot be exchanged until the authentication procedure is completed. Total "security originated" delay affects the network's data throughput, especially when data are broadcast to several nodes for routing and retransmission purposes.

1. Node Authentication Delay

The total node authentication delay, t_{total}, can be derived by first examining the individual algorithms presented in Chapter III (see Figures 14 and 15) to determine the delays associated with the authentication request, $t_{req,}$ and the authentication response, t_{res}. These can be shown to be

$$t_{req} = t_{ID\text{-}Hash} + t_{enc\ Hash\text{-}pri} + t_{enc\ ID\text{-}K} + t_{enc\ K\text{-}pub} \tag{4.1}$$

$$t_{res} = t_{dec\_K\_pri} + t_{dec\_ID\_K} + t_{dec\_H(ID)\_pub} + t_{ID\text{-}Hash} \tag{4.2}$$

where $t_{ID\text{-}Hash}$ is the time required for the ID to be hashed, $t_{enc\ Hash\text{-}pri}$ is the time required to encrypt the hash with the private key, $t_{enc\ ID\text{-}K}$ is the time required to encrypt the ID with the selected key K and $t_{enc\ K\text{-}pub}$ is the time required to encrypt the key with a public key. Similarly, $t_{dec\_K\_pri}$, $t_{dec\_ID\_K}$, $t_{dec\_H(ID)\_pub}$ and t_{ID_Hash} represent the time required for

the decryption process of the authenticator. These terms are summed and the total is doubled to include both the centralized and distributed authentication stages to arrive at

$$t_{total} = 2 \times (t_{req} + t_{res}) . \tag{4.3}$$

2. Data Authentication

In this section, we evaluate the TESLA key disclosure parameter, *d*, for a hybrid large-scale wireless sensor network. It is desirable to minimize *d* to improve the real-time dissemination performance of the mechanism. Overall performance analysis of the implementation of the TESLA algorithm can be found in [15]. TESLA accommodates variable packet flow rates by determining *d* for each chain. Multiple chains allow the binding of links with different channel characteristics (e.g., propagation delay and transmission rate). As given in (3.1), *d* is proportional to the maximum synchronization error between the sender and the receiver and the maximum network propagation delay. Larger values of *d* increase the authentication time because the receiver will have to buffer all the received packets until the appropriate authentication key is received. The parameter *d* must be chosen to be greater than the total transmission time for each link between the sender and the receiver. Otherwise, packets would be dropped as invalid and the performance of the algorithm would be degraded. Additionally, it can be seen that a reduction in the maximum synchronization error allows for a commensurate reduction in *d*. Assumed that a GPS time signal is used for synchronization among all nodes, then the time synchronization error will be on order of 100 ns [28].

3. Simulation Results

In this section, the delay performance of our node authentication algorithm is evaluated on a 3.4 GHz Pentium IV Windows PC in Java using the library of cryptographic functions provided by the GNU Crypto project [6]. A C/C++ implementation may prove to be faster, but the results produced by the JAVA implementation provide a relative comparison of the performance of the algorithm.

At this point, we simulate a new node entering the network and both the proposed centralized and the distributed algorithms are applied. The Java cryptographic library is capable of measuring decryption and encryption times for several symmetric algorithms and hash functions. An example of the output of the Java execution code is shown in Figure 18. In this example, the input data was a 10-byte packet, and the program measured encryption and decryption times of several symmetric algorithms as well as the performance of different hash functions.

Additional time required for the generation of the private and public keys for the new node is not included in the total authentication time since it is assumed that the command and control node (authenticator) has pre-computed several sets of keys for this purpose before the authentication process has started.

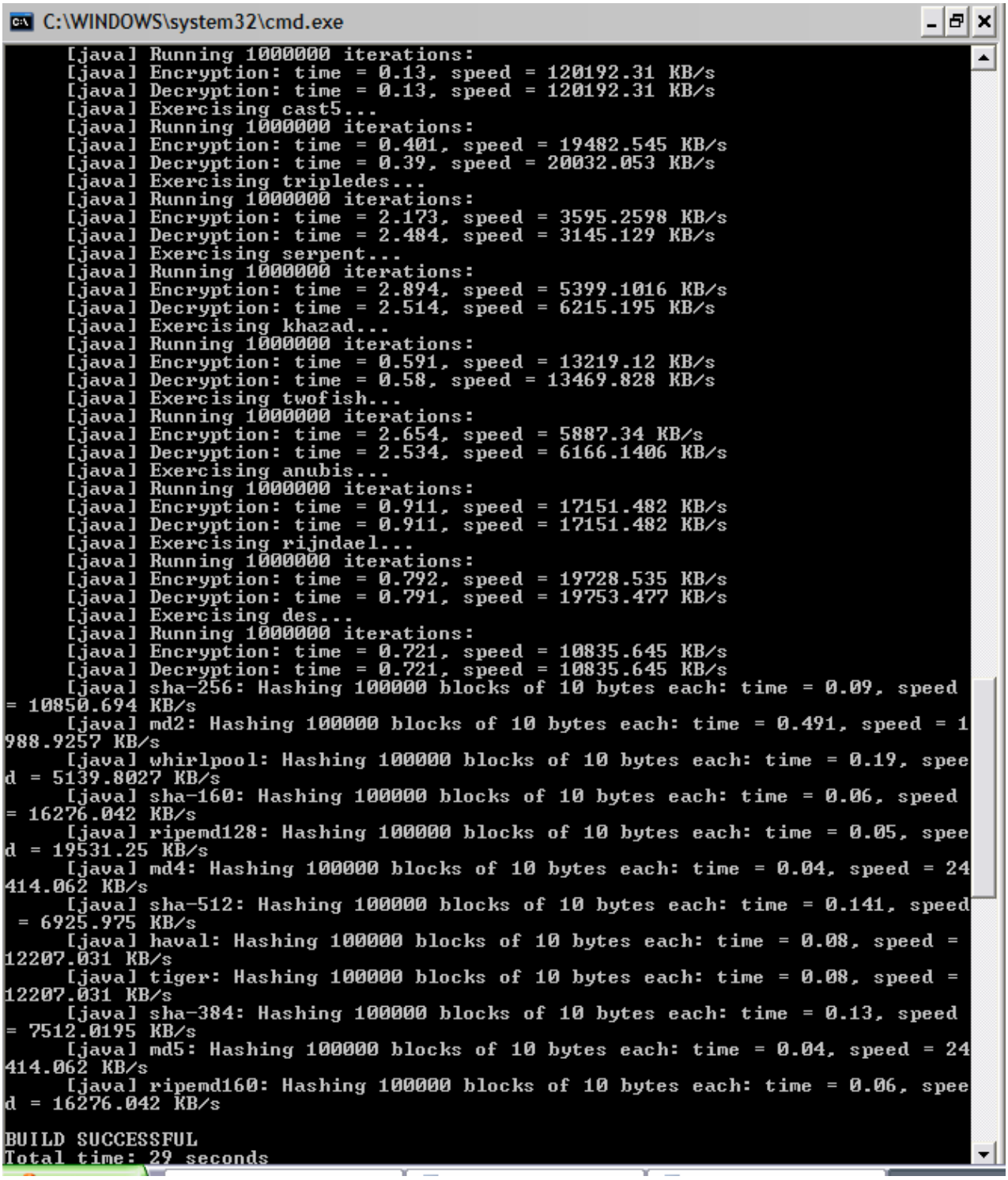
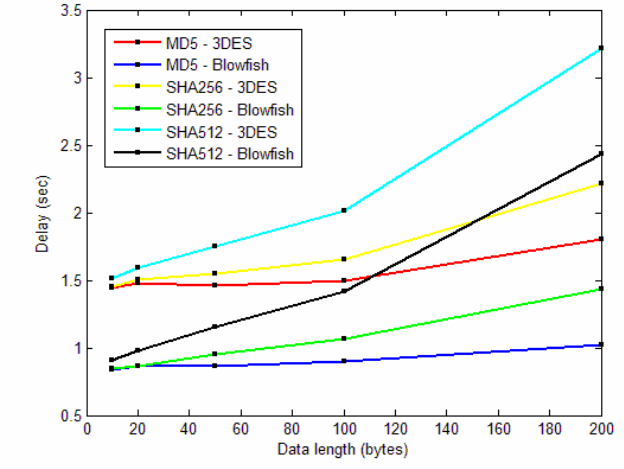
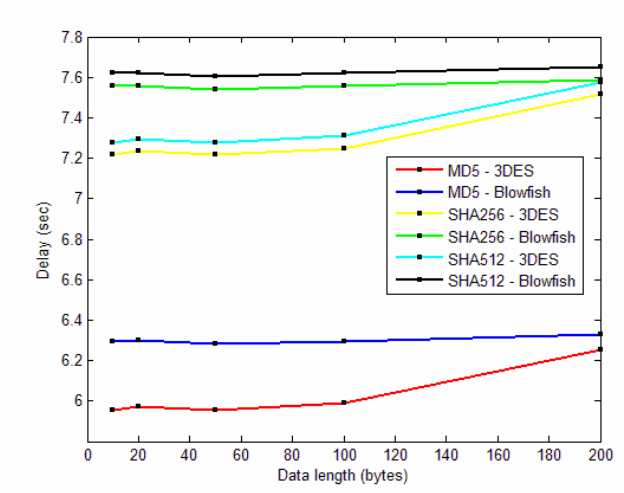

C:\WINDOWS\system32\cmd.exe
[java] Running 1000000 iterations:
[java] Encryption: time = 0.13, speed = 120192.31 KB/s
[java] Decryption: time = 0.13, speed = 120192.31 KB/s
[java] Exercising cast5...
[java] Running 1000000 iterations:
[java] Encryption: time = 0.401, speed = 19482.545 KB/s
[java] Decryption: time = 0.39, speed = 20032.053 KB/s
[java] Exercising tripledes...
[java] Running 1000000 iterations:
[java] Encryption: time = 2.173, speed = 3595.2598 KB/s
[java] Decryption: time = 2.484, speed = 3145.129 KB/s
[java] Exercising serpent...
[java] Running 1000000 iterations:
[java] Encryption: time = 2.894, speed = 5399.1016 KB/s
[java] Decryption: time = 2.514, speed = 6215.195 KB/s
[java] Exercising khazad...
[java] Running 1000000 iterations:
[java] Encryption: time = 0.591, speed = 13219.12 KB/s
[java] Decryption: time = 0.58, speed = 13469.828 KB/s
[java] Exercising twofish...
[java] Running 1000000 iterations:
[java] Encryption: time = 2.654, speed = 5887.34 KB/s
[java] Decryption: time = 2.534, speed = 6166.1406 KB/s
[java] Exercising anubis...
[java] Running 1000000 iterations:
[java] Encryption: time = 0.911, speed = 17151.482 KB/s
[java] Decryption: time = 0.911, speed = 17151.482 KB/s
[java] Exercising rijndael...
[java] Running 1000000 iterations:
[java] Encryption: time = 0.792, speed = 19728.535 KB/s
[java] Decryption: time = 0.791, speed = 19753.477 KB/s
[java] Exercising des...
[java] Running 1000000 iterations:
[java] Encryption: time = 0.721, speed = 10835.645 KB/s
[java] Decryption: time = 0.721, speed = 10835.645 KB/s
[java] sha-256: Hashing 100000 blocks of 10 bytes each: time = 0.09, speed = 10850.694 KB/s
[java] md2: Hashing 100000 blocks of 10 bytes each: time = 0.491, speed = 1988.9257 KB/s
[java] whirlpool: Hashing 100000 blocks of 10 bytes each: time = 0.19, speed = 5139.8027 KB/s
[java] sha-160: Hashing 100000 blocks of 10 bytes each: time = 0.06, speed = 16276.042 KB/s
[java] ripemd128: Hashing 100000 blocks of 10 bytes each: time = 0.05, speed = 19531.25 KB/s
[java] md4: Hashing 100000 blocks of 10 bytes each: time = 0.04, speed = 24414.062 KB/s
[java] sha-512: Hashing 100000 blocks of 10 bytes each: time = 0.141, speed = 6925.975 KB/s
[java] haval: Hashing 100000 blocks of 10 bytes each: time = 0.08, speed = 12207.031 KB/s
[java] tiger: Hashing 100000 blocks of 10 bytes each: time = 0.08, speed = 12207.031 KB/s
[java] sha-384: Hashing 100000 blocks of 10 bytes each: time = 0.13, speed = 7512.0195 KB/s
[java] md5: Hashing 100000 blocks of 10 bytes each: time = 0.04, speed = 24414.062 KB/s
[java] ripemd160: Hashing 100000 blocks of 10 bytes each: time = 0.06, speed = 16276.042 KB/s
BUILD SUCCESSFUL
Total time: 29 seconds

Figure 18. JAVA code execution demo

Figures 19 and 20 illustrate the performance of our proposed node authentication algorithm. For this simulation, we used several data lengths and the total authentication delay t_{total}. The individual request and response times, t_{req} and t_{res}, respectively, are plotted as a function of the data length. The performance of all the cryptographic mechanisms is directly related to the computational power of the source and the destination. Faster processors will achieve lower encryption and decryption delays. Nevertheless, the results are representative, and it can be seen that reasonable latency is achieved even with the limited processing power obtained from a lab PC.



(a)



(b)

Figure 19. Node authentication delays (t_{req} and t_{res}) for (a) encryption and (b) decryption

Closely examining the terms in t_{req} and t_{res} , it is observed that the length of the key size in the RSA algorithm (used to encrypt/decrypt the hash of the ID and the random key) is the dominating factor in the total authentication delay of our algorithm. The low encryption and decryption performance of the asymmetric algorithms compared to the symmetric algorithms [23] increases the total authenticators delay. A RSA key length of 1024 bits, a Blowfish key length of 448 bits and a 3DES key length of 158 bits were used in the simulation. All cryptographic processes are assumed to be executed sequentially. Parallel processing techniques could further improve the performance of the proposed algorithm.

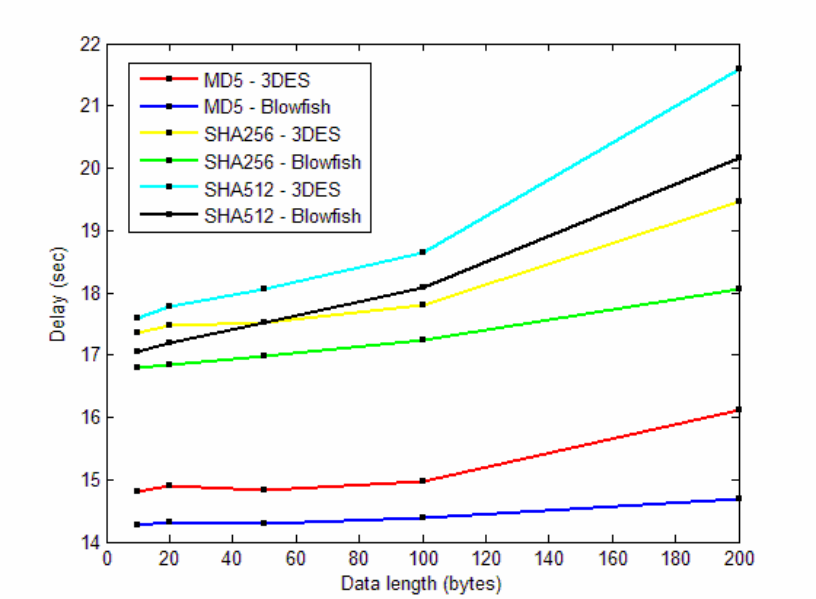


Figure 20. Total node authentication delay (t_{total})

Although it can be seen that, in general, larger keys result in longer delays, the use of efficient algorithms, such as Blowfish, can produce dramatic improvements in encryption delay times. As anticipated, in all cases, the RSA algorithm key is seen to be the dominant factor. Further, the use of an algorithm with a large key size, such as Blowfish in our scenario, dramatically increases the decryption time because a public key decryption process is performed to reveal this key. The effect is more visible when it is combined with the choice of a hash function, such as SHA512, with a large output.

B. DATA CONFIDENTIALITY

The data confidentiality mechanism ensures that the exchanged data can only be viewed and processed by legitimate users of the network. In our proposed solution, data confidentiality is accomplished using the IPSec protocol suite. In this section, an OPNET simulation is performed to examine IPSec performance in the context of a hybrid, large-scale network for missile defense.

1. OPNET Implementation

We used the OPNET network simulator to simulate the hybrid, large-scale network. The network topology is depicted in Figure 21.

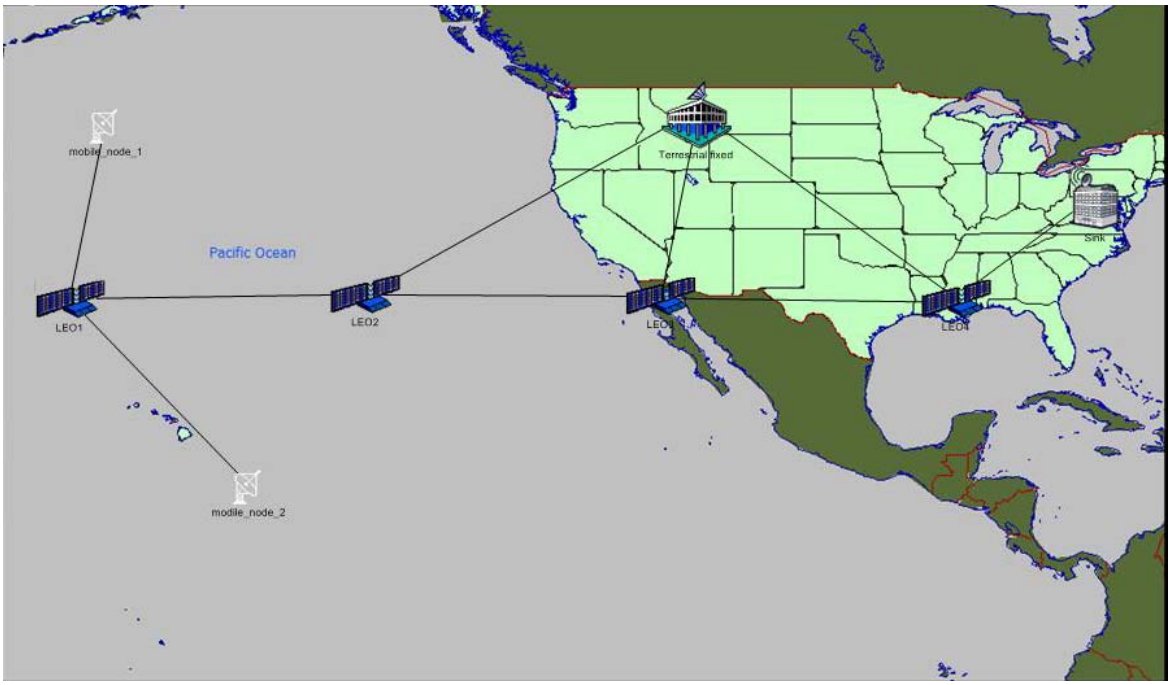


Figure 21. OPNET network topology

Our simulated network consists of 8 nodes: two mobile terrestrial nodes, four satellites, and two fixed terrestrial nodes. These were comprised of four LEO satellites, one X-band radar, one war ship, and two ground stations exchanging target data. It is assumed that tracking has commenced; therefore, the GEO satellites are not modeled in

the simulator. It is envisioned that the GEO satellites will be used for initial viewing only due to the large propagation distances and the lack of on board tracking sensors. The eastern ground station simulated the Command and Control Center (Sink), which collects all the unprocessed target data. Each node is interconnected by a point-to-point link, configured to simulate a wireless channel. The OSPF protocol was used for routing. Node and channel configuration characteristics are shown in Table 7.

Links	BER: 10^{-4}	Data Rate (R): 2 Mbps
Mobile nodes	Data length (L): 100 bytes,	Packet inter-arrival time: promoted (set to 13 different PRFs)
Satellite nodes	Altitude: 1000 km,	Distance between LEOs: 2200 km

Table 7. OPNET simulation parameters

In this simulation, we assume that target data are generated by Mobile Node 1 and the RF sensor (X-band radar). In the equivalent scenario, these two network nodes are tracking the incoming ballistic missile target and are sending target data to the command and control node for further processing. Data are sent at a rate proportional to the PRF value of the tracking radar. The total delay is measured at the sink (the command and control node).

Traffic generators are properly configured to create IPSec packets. An IPSec process module has been installed and set to use ESP packet formats in transport mode. Each ESP packet uses HMAC-MD5-96 for authentication and AES in CBC mode (128 bits each block) with a key size of 128 bits for encryption. The average authentication and encryption times of the algorithms are calculated and inserted as processing delays in the IPSec process model.

2. Simulation Results

Figure 22 plots the total average delay for IP and IPSec as a function of PRF. From the plot, the latency associated with IPSec can be clearly seen. The increase in delay for IPSec, though, is less than 3% of the total end-to-end latency.

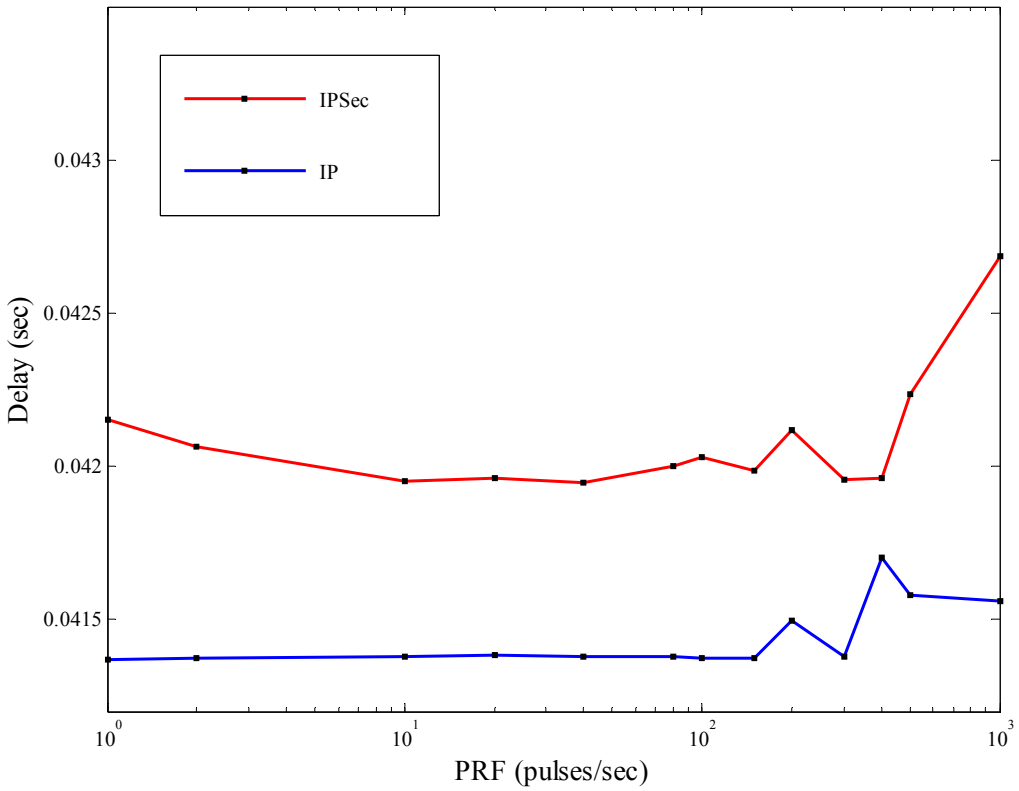


Figure 22. Average delay versus PRF

The delay presented in this graph is produced by 8 nodes. We expect an increase of the total delay when larger geographical areas are covered, or when the number of the participating nodes is increased.

Figure 23 presents a comparison of the throughput at the receiver node (Sink) for both IP and IPSec scenarios as a function of PRF. The decrease in throughput for IPSec is due to the overhead that IPSec introduces. An ESP packet adds an overhead of almost 32-36 bytes for each IP packet (as shown in Figure 10). The overall throughput could be increased through the use of data aggregation.

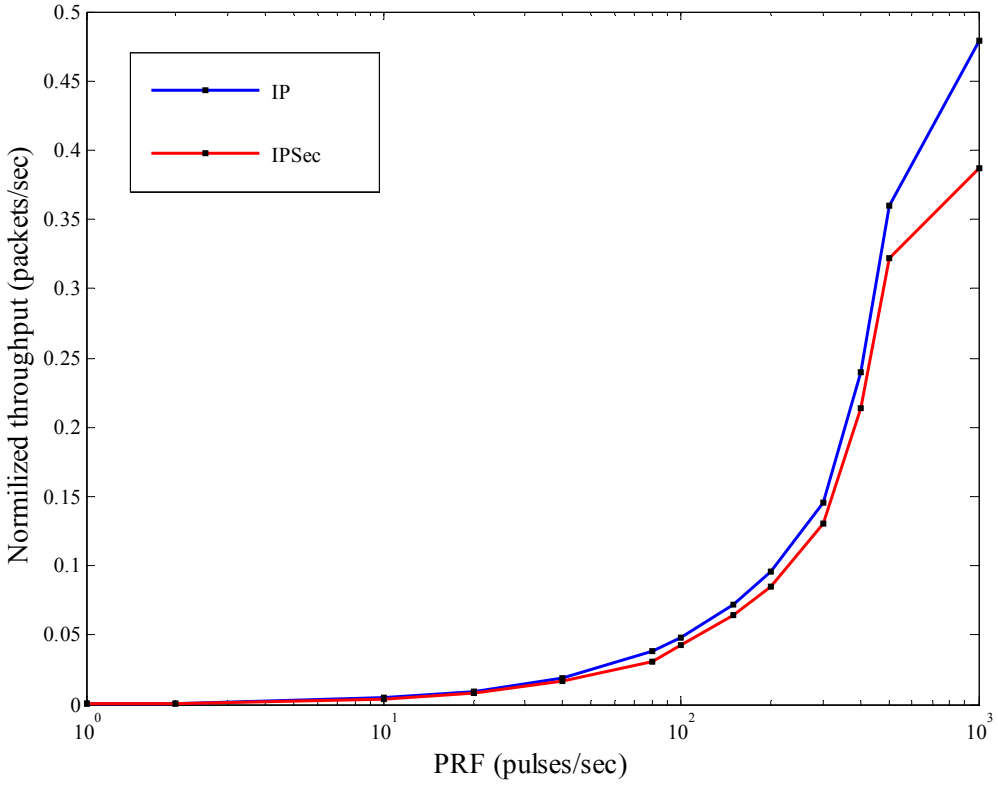


Figure 23. Throughput versus PRF

C. SUMMARY

This chapter provided performance analysis and simulation of the proposed security scheme for authentication and confidentiality. Using the GNU Java cryptographic library, encryption and decryption times for the multistage node authentication scenario were calculated. The associated total delay proved to be reasonable and will be further improved because the processing capabilities of the actual nodes exceed those of the lab PC used for the simulation. Larger key lengths were seen to improve security with the trade-off of longer delays. An OPNET simulation was developed to measure the total delay when IPSec is implemented. It was shown that the additional delay of the IPSec implementation was reasonable when compared to the overall latency of the IP.

V. CONCLUSIONS

This thesis proposed multistage security mechanism for a hybrid, large-scale wireless sensor network designed to support the integrated ballistic missile defense system. This scheme combines node and data authentication mechanisms to provide robust security coupled with real-time data dissemination and utilizes data encryption to ensure data confidentiality. Performance and simulation analysis demonstrated that the delay and throughput of the proposed system commensurate with unencrypted IP.

A. CONTRIBUTIONS OF THIS THESIS

This thesis accomplished two objectives. Firstly, a robust, real-time secure authentication mechanism was proposed. Node authentication was provided in two stages using RSA with the result that the new node obtained authentication credentials from two separate authenticators. The algorithm makes use of digital signatures and certificates to ensure that only legitimate nodes will enter the network. Data authentication and confidentiality were accomplished through the implementation of the TESLA algorithm and the IPSec set of protocols, respectively. TESLA exhibited packet loss tolerance and provided secure data authentication. It can accommodate multiple data rates interconnecting various types of links. IPSec encrypts transmitted data, protecting the valuable content from unauthorized viewing. In our solution, it is applied at the IP layer and is application transparent.

Secondly, performance analysis and simulation were performed to verify that the overhead introduced by the security mechanism did not substantially impact network throughput and delay. The RSA algorithm key length is an essential design and implementation parameter for our proposed algorithm since it dominates the delay performance of the node authentication mechanism. The trade-off between increased security and end-to-end latency was identified and evaluated through both analysis and simulation.

B. RECOMMENDATIONS FOR FUTURE WORK

This thesis proposed a real-time multistage security mechanism to support the hybrid, large-scale wireless sensor networks for missile defense. It combined node authentication based on digital signatures and the public key infrastructure (PKI) and data authentication using the time efficient stream loss-tolerant authentication (TESLA) protocol. The proposed mechanism also utilizes data encryption (IPSec) to provide data confidentiality.

The analysis of the disclosing parameter *d* of the TESLA algorithm was performed only based on link characteristics. Only a lower bound was evaluated, without any further investigation. Additionally, the performance of the security mechanism was demonstrated using sequential processing of the associated cryptographic functions. Moreover, the proposed mechanism addressed only authentication and confidentiality issues.

Future work should include a complete implementation and subsequently fielding of the security mechanism proposed. As part of this follow-on work, the analysis of disclosing parameter *d* of the TESLA algorithm should be expanded. Additional improvements to the performance of the security mechanism, including parallel processing and data aggregation within the AOI, may be investigated. A complete security solution would also address other security challenges, such as defending against denial of service (DoS) and other types of attacks, detecting misbehaving or rogue nodes, preventing traffic analysis, and optimizing key management techniques.

LIST OF REFERENCES

1. A. Roy-Chowdhury, J.S. Baras, M. Hadjitheodosiou, S. Papademetriou, "Security Issues In Hybrid Networks With a Satellite Component," *IEEE Wireless Communications, December 2005*, Volume 12, Issue 6, December 2005, pp. 50 – 61.

2. J. Border, M. Kojo, J. Griner, G. Montenegro, Z. Shelby, "Performance Enhancing Proxies Intended to Mitigate Link-Related Degradations," RFC 3135, June 2001.

3. E.L. Dereniak, G.D. Boreman, *"Infrared Detectors and Systems,"* Wiley, 1996.

4. W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, November 1976, pp. 644-654.

5. D. Demirel, F. Alagoz, M. U. Qaglayan, "IPSEC over Satellite Links: A New Flow Identification Method," *International Symposium on Computer Networks 2006*, pp. 140 – 146, June 2006.

6. The GNU Crypto Project – Free Software Foundation, http://www.gnu.org/software/gnu-crypto/, February 2007.

7. S. D. Gunapala and S. V. Bandara, "Quantum Well Infrared Photo-detector (QWIP) Focal Plane Arrays," Center for Space Microelectronics Technology, Jet Propulsion Laboratory, California Institute of Technology, published in "Semiconductors and Semimetals" series, Vol. 62, 1999.

8. P. Katopodis, Gr. Katsis, O. Walker, M. Tummala, J. B. Michael, "Hybrid large scale wireless sensor network for missile defense," *In Proc. IEEE International Conference of SoSE*, San Antonio, TX, April 2007.

9. Gr. Katsis, P. Katopodis, T.O. Walker III, M. Tummala, J. B. Michael, "Multistage authentication for hybrid large scale mobile wireless sensor networks for missile defense," *Submitted for publication in the 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'07)*, Athens Greece, September 2007.

10. N. Koblitz, *"Elliptic curve cryptosystems,"* in Mathematics of Computation 48, 1987, pp. 203–209.

11. J. Kong, "Providing Robust and Ubiquitous Security Support for Mobile Ad Hoc Networks," *In Proc. 9th Int'l Conf. Network Protocols (ICNP'01)*, 2001, pp. 579-89.

12. M. Luk, A. Perrig and B. Whillock, "Seven cardinal properties of sensor network broadcast authentication," *In Proceedings of the Fourth ACM Workshop on Security of Ad Hoc and Sensor Networks SASN '06*, 2006, pp. 147-156.

13. Missile Defense Agency (MDA), *"Ballistic Missile Defense System Overview (BDMS),"* 15 March 2005.

14. Quantum Well Infrared Photodetector (QWIP) Home Page, Jet Propulsion Laboratory, http://qwip.jpl.nasa.gov/, April 2007.

15. A. Perrig, R. Canetti, J. D. Tygar and S. Dawn, "Efficient authentication and signing of multicast streams over lossy channels," In *Proceedings of the 2000 IEEE Symposium on Security and Privacy*, May 2000, pp. 56-73.

16. A. Perrig, "The BiBa one-time signature and broadcast authentication protocol," I*n Proceedings of the Eighth ACM Conference on Computer and Communications Security (CSS-8)*, Philadelphia, PA, November 2001, pp. 28-37.

17. A. Perrig, R. Canetti, D. Tygar and D. Song, "The TESLA Broadcast Authentication Protocol," CryptoBytes, vol. 5, Summer 2002.

18. A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen and D. E. Culler, "SPINS: Security Protocols for Sensor Networks," Wireless Networks, vol. 8, p. 521, September 2002.

19. L. Reyzin, N. Reyzin, "Better than BiBa: Short onetime signatures with fast signing and verifying," *In Seventh Australasian Conference on Information Security and Privacy (ACISP 2002)*, July 2002.

20. R. L. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun ACM, vol. 21, pp. 120-126, 1978.

21. K. Sankar, S. Sundaralingam, A. Balinsky and D. Miller, *"Cisco wireless LAN security,"* Scitech Book News, vol. 30, pp. 13-34, September 2006.

22. S. Chang, S. Shieh, W. W. Lin, C. Hsieh, "An Efficient Broadcast Authentication Scheme in Wireless Sensor Networks," *In Proceedings of the 2006 ACM Symposium on Information, computer and communications security ASIACCS '06*, March 2006.

23. W. Stallings, *"Cryptography and Network Security,"* Fourth ed., Prentice Hall, November 2005.

24. M.Z. Tidrow, W.R. Dyer, "Infrared Sensors for ballistic missile defense," (Ballistic Missile Defense Organization, Pentagon Washington, D.C.), Infrared Science & Technology, published by Elsevier Science B.V., 2001.

25. M.Z. Tidrow, “New infrared sensors for ballistic missile defense,”(Missile Defense Agency/Advanced Systems, Pentagon Washington DC), Quantum Sensing and Nanophotonic Devices II, *In Proceedings of SPIE Vol. 5732*, Bellingham, WA, 2005.

26. I.R. Thompson, A.O. Waller, G. Jones, **“**Performance Enhancing Proxies and Security,” *IEEE Seminar on IP over Satellite*, The Next Generation: MPLS, VPN and DRM Delivered Services, 2003, pp. 1- 14.

27. K. Uzun, Master’s thesis, “Requirements and limitations of boost-phase ballistic missiles intercept systems,” Naval Postgraduate School, September 2004.

28. T.O. Walker III; M. Tummala, J.B. Michael, **“**Pulse transmission scheduling for a distributed system of cooperative radars,” *2006 IEEE/SMC International Conference on System of Systems Engineering*, Los Angeles, 24-26 April 2006, 6 pp.

29. D.A. Wilkening, “*Airborne Boost-Phase Ballistic Missile Defense,”* Science and Global Security, Taylor & Francis, Vol. 12, pp. 1-67, 2004.

30. P. Woodward, T. Pell, G. Hernandez, “Performance enhancing proxies - are they as beneficial as they seem,” *IEEE Seminar on IP over Satellite*, The Next Generation: MPLS, VPN and DRM Delivered Services, 2003, pp. 22-26.

31. S. Yi, R. Kravets, “Key Management for Heterogeneous Ad Hoc Wireless Networks,” University of Illinois at Urbana-Champaign, 2002.

32. S. Yi, R. Kravets, “MOCA: Mobile Certificate Authority for Wireless Ad Hoc Networks,” Report No. UIUCDCS-R-2004-2502, UILU-ENG-2004-1805, University of Illinois at Urbana-Champaign, 2002.

33. Z, Wang; Q. Guo; X. Gu, “Comprehensive Computational Analysis on TCP in Satellite Links,” *Innovative Computing Information and Control 2006, ICICIC06*, Volume 1, 30-01, pp. 716 – 721, August 2006.

34. L. Zhu, Z.J. Haas, “Securing Ad Hoc Networks,” IEEE Network Mag., vol. 13, no. 6, November/December 1999, pp. 24-30.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Professor Jeffrey B. Knorr
   Chairman, Department of Electrical and Computer Engineering
   Naval Postgraduate School
   Monterey, California

4. Professor James H. Luscombe
   Chairman, Department of Physics
   Naval Postgraduate School
   Monterey, California

5. Professor Murali Tummala
   Department of Electrical and Computer Engineering
   Naval Postgraduate School
   Monterey, California

6. Associate Professor Gamani Karunasiri
   Department of Physics
   Naval Postgraduate School
   Monterey, California

7. Professor J. Bret Michael
   Department of Electrical and Computer Engineering
   Naval Postgraduate School
   Monterey, California

8. CDR Owens Walker USN
   Department of Electrical and Computer Engineering
   Naval Postgraduate School
   Monterey, California

9. Ms. Deborah Stiltner
   Missile Defense National Team
   Crystal City, Virginia

10. Hellenic Navy, General Staff
Athens, Greece

11. LT Grigorios Katsis
Department of Physics
Naval Postgraduate School
Monterey, California